



## **Cisco ME 3400E Ethernet Access Switch Command Reference**

Cisco IOS Release 12.2(58)SE  
April 2011

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast,

**Americas Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

Text Part Number: OL-16486-05

EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

*Cisco ME 3400E Ethernet Access Switch Command Reference*

© 2011 Cisco Systems, Inc. All rights reserved.



## CONTENTS

### **Preface** xix

Audience xix

Purpose xix

Conventions xx

Filtering **show** Command Output xx

Related Publications xx

Obtaining Documentation and Submitting a Service Request xxi

---

### CHAPTER 1

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

CLI Command Modes 1-1

User EXEC Mode 1-2

Privileged EXEC Mode 1-3

Global Configuration Mode 1-3

Interface Configuration Mode 1-4

VLAN Configuration Mode 1-4

Line Configuration Mode 1-4

---

### CHAPTER 2

### **Cisco ME 3400E Ethernet Access Switch**

#### **Cisco IOS Commands** 2-1

aaa accounting dot1x 2-1

aaa authentication dot1x 2-3

action 2-5

alarm-contact 2-7

archive download-sw 2-9

archive tar 2-12

archive upload-sw 2-15

arp access-list 2-17

bandwidth 2-19

boot buffersize 2-22

boot config-file 2-23

boot enable-break 2-24

boot helper 2-25

boot helper-config-file 2-26

boot manual	2-27
boot private-config-file	2-28
boot system	2-29
channel-group	2-30
channel-protocol	2-34
class	2-36
class-map	2-38
clear ip arp inspection log	2-40
clear ip arp inspection statistics	2-41
clear ip dhcp snooping	2-42
clear ipc	2-44
clear ipv6 dhcp conflict	2-45
clear l2protocol-tunnel counters	2-46
clear lacp	2-47
clear logging onboard	2-48
clear mac address-table	2-49
clear mac address-table move update	2-50
clear pagp	2-51
clear policer cpu uni-eni counters	2-52
clear port-security	2-53
clear rep counters	2-55
clear spanning-tree counters	2-56
clear spanning-tree detected-protocols	2-57
clear vmps statistics	2-59
conform-action	2-60
copy logging onboard module	2-62
cpu traffic qos cos	2-64
cpu traffic qos dscp	2-68
cpu traffic qos precedence	2-73
cpu traffic qos qos-group	2-76
define interface-range	2-78
delete	2-80
deny (ARP access-list configuration)	2-81
deny (IPv6 access-list configuration)	2-83
deny (MAC access-list configuration)	2-89

diagnostic monitor	2-92
diagnostic schedule test	2-94
diagnostic start test	2-96
dot1x default	2-98
dot1x host-mode	2-99
dot1x initialize	2-101
dot1x max-reauth-req	2-102
dot1x max-req	2-104
dot1x port-control	2-105
dot1x re-authenticate	2-107
dot1x reauthentication	2-108
dot1x supplicant force-multicast	2-109
dot1x system-auth-control	2-110
dot1x test eapol-capable	2-111
dot1x test timeout	2-112
dot1x timeout	2-113
dot1x violation-mode	2-115
duplex	2-116
errdisable detect cause	2-118
errdisable recovery	2-120
ethernet dot1ad	2-122
ethernet evc	2-124
ethernet lmi	2-125
ethernet lmi ce-vlan map	2-127
ethernet loopback (interface configuration)	2-129
ethernet loopback (privileged EXEC)	2-132
ethernet oam remote-failure	2-134
ethernet uni	2-136
ethernet uni id	2-138
exceed-action	2-139
flowcontrol	2-141
hw-module module logging onboard	2-143
interface port-channel	2-145
interface range	2-147
interface vlan	2-149

ip access-group	2-151
ip address	2-154
ip arp inspection filter vlan	2-156
ip arp inspection limit	2-158
ip arp inspection log-buffer	2-160
ip arp inspection trust	2-162
ip arp inspection validate	2-163
ip arp inspection vlan	2-165
ip arp inspection vlan logging	2-166
ip device tracking maximum	2-168
ip dhcp snooping	2-169
ip dhcp snooping binding	2-170
ip dhcp snooping database	2-172
ip dhcp snooping information option	2-174
ip dhcp snooping information option allowed-untrusted	2-176
ip dhcp snooping information option format remote-id	2-178
ip dhcp snooping limit rate	2-179
ip dhcp snooping trust	2-180
ip dhcp snooping verify mac-address	2-181
ip dhcp snooping vlan	2-182
ip dhcp snooping vlan information option format-type circuit-id string	2-183
ip igmp filter	2-185
ip igmp max-groups	2-187
ip igmp profile	2-189
ip igmp snooping	2-191
ip igmp snooping last-member-query-interval	2-193
ip igmp snooping querier	2-195
ip igmp snooping report-suppression	2-197
ip igmp snooping tcn	2-199
ip igmp snooping tcn flood	2-200
ip igmp snooping vlan immediate-leave	2-201
ip igmp snooping vlan mrouter	2-202
ip igmp snooping vlan static	2-204
ip sla responder twamp	2-206
ip sla server twamp	2-208

ip source binding	2-210
ip ssh	2-212
ip sticky-arp (global configuration)	2-214
ip sticky-arp (interface configuration)	2-216
ip verify source	2-218
ipv6 access-list	2-220
ipv6 address dhcp	2-222
ipv6 dhcp client request vendor	2-223
ipv6 dhcp ping packets	2-224
ipv6 dhcp pool	2-225
ipv6 dhcp server	2-228
ipv6 mld snooping	2-230
ipv6 mld snooping last-listener-query-count	2-232
ipv6 mld snooping last-listener-query-interval	2-234
ipv6 mld snooping listener-message-suppression	2-236
ipv6 mld snooping robustness-variable	2-237
ipv6 mld snooping tcn	2-239
ipv6 mld snooping vlan	2-241
ipv6 traffic-filter	2-243
l2protocol-tunnel	2-245
l2protocol-tunnel cos	2-248
lacp port-priority	2-249
lacp system-priority	2-251
link state group	2-253
link state track	2-255
location (global configuration)	2-256
location (interface configuration)	2-258
logging event	2-260
logging file	2-261
mac access-group	2-263
mac access-list extended	2-265
mac address-table aging-time	2-267
mac address-table learning vlan	2-268
mac address-table move update	2-270
mac address-table notification	2-272

mac address-table static	2-274
mac address-table static drop	2-275
macro apply	2-277
macro description	2-279
macro global	2-280
macro global description	2-282
macro name	2-283
match (access-map configuration)	2-285
match access-group	2-287
match cos	2-288
match dot1ad dei	2-290
match ip dscp	2-292
match ip precedence	2-294
match qos-group	2-296
match vlan	2-298
mdix auto	2-301
media-type	2-303
monitor session	2-305
mvr (global configuration)	2-309
mvr (interface configuration)	2-312
no authentication logging verbose	2-315
no dot1x logging verbose	2-316
no mab logging verbose	2-317
oam protocol cfm svlan	2-318
pagp learn-method	2-319
pagp port-priority	2-321
permit (ARP access-list configuration)	2-323
permit (IPv6 access-list configuration)	2-325
permit (MAC access-list configuration)	2-330
police	2-333
policer aggregate (global configuration)	2-338
police aggregate (policy-map class configuration)	2-343
policer cpu uni	2-345
policy-map	2-347
port-channel load-balance	2-350



port-type	2-352
power-supply dual	2-354
priority	2-356
private-vlan	2-359
private-vlan mapping	2-362
queue-limit	2-364
remote-span	2-367
renew ip dhcp snooping database	2-369
rep admin vlan	2-370
rep block port	2-371
rep lsl-age-timer	2-375
rep preempt delay	2-377
rep preempt segment	2-379
rep segment	2-380
rep stcn	2-383
reserved-only	2-384
rmon collection stats	2-385
sdm prefer	2-386
service instance	2-389
service password-recovery	2-391
service-policy (interface configuration)	2-393
service-policy (policy-map class configuration)	2-395
set cos	2-397
set dot1ad dei	2-399
set dscp	2-401
set precedence	2-403
set qos-group	2-405
setup	2-407
shape average	2-410
show access-lists	2-412
show archive status	2-415
show arp access-list	2-416
show boot	2-417
show cable-diagnostics tdr	2-419
show class-map	2-421

show controllers cpu-interface	2-422
show controllers ethernet-controller	2-424
show controllers tcam	2-431
show controllers utilization	2-433
show cpu traffic qos	2-435
show diagnostic	2-437
show dot1q-tunnel	2-441
show dot1x	2-442
show env	2-445
show errdisable detect	2-447
show errdisable flap-values	2-449
show errdisable recovery	2-451
show etherchannel	2-453
show ethernet loopback	2-456
show ethernet service evc	2-458
show ethernet service instance	2-459
show ethernet service interface	2-461
show flowcontrol	2-463
show idprom	2-465
show interfaces	2-467
show interfaces counters	2-475
show interfaces rep	2-477
show interfaces transceivers	2-479
show inventory	2-482
show ip arp inspection	2-483
show ip dhcp snooping	2-487
show ip dhcp snooping binding	2-488
show ip dhcp snooping database	2-490
show ip dhcp snooping statistics	2-492
show ip igmp profile	2-497
show ip igmp snooping	2-498
show ip igmp snooping groups	2-500
show ip igmp snooping mrouter	2-502
show ip igmp snooping querier	2-503
show ip sla standards	2-505

show ip sla twamp connection	2-506
show ip sla twamp session	2-508
show ip source binding	2-509
show ip verify source	2-510
show ipc	2-512
show ipv6 access-list	2-516
show ipv6 dhcp conflict	2-518
show ipv6 route updated	2-519
show l2protocol-tunnel	2-521
show lacp	2-523
show link state group	2-527
show location	2-529
show logging onboard	2-532
show mac access-group	2-536
show mac address-table	2-537
show mac address-table address	2-539
show mac address-table aging-time	2-540
show mac address-table count	2-542
show mac address-table dynamic	2-544
show mac address-table interface	2-546
show mac address-table learning	2-548
show mac address-table move update	2-549
show mac address-table notification	2-550
show mac address-table static	2-552
show mac address-table vlan	2-554
show monitor	2-556
show mvr	2-558
show mvr interface	2-560
show mvr members	2-562
show pagp	2-564
show parser macro	2-566
show policer aggregate	2-568
show policer cpu uni-eni	2-569
show policy-map	2-572
show port-security	2-577

show port-type 2-580

show rep topology 2-582

show sdm prefer 2-585

show spanning-tree 2-587

show storm-control 2-593

show system mtu 2-595

show table-map 2-596

show udld 2-597

show version 2-600

show vlan 2-602

show vlan access-map 2-607

show vlan filter 2-608

show vlan mapping 2-609

show vmps 2-611

shutdown 2-613

shutdown vlan 2-614

snmp mib rep trap-rate 2-615

snmp-server enable traps 2-616

snmp-server host 2-620

snmp trap mac-notification change 2-624

spanning-tree 2-626

spanning-tree bpdfilter 2-628

spanning-tree bpdguard 2-630

spanning-tree cost 2-632

spanning-tree etherchannel guard misconfig 2-634

spanning-tree extend system-id 2-636

spanning-tree guard 2-638

spanning-tree link-type 2-640

spanning-tree loopguard default 2-642

spanning-tree mode 2-644

spanning-tree mst configuration 2-646

spanning-tree mst cost 2-648

spanning-tree mst forward-time 2-650

spanning-tree mst hello-time 2-651

spanning-tree mst max-age 2-653

spanning-tree mst max-hops	2-655
spanning-tree mst port-priority	2-657
spanning-tree mst pre-standard	2-659
spanning-tree mst priority	2-660
spanning-tree mst root	2-662
spanning-tree port-priority	2-664
spanning-tree portfast (global configuration)	2-666
spanning-tree portfast (interface configuration)	2-669
spanning-tree vlan	2-671
speed	2-674
storm-control	2-676
switchport	2-679
switchport access vlan	2-681
switchport backup interface	2-683
switchport block	2-687
switchport host	2-689
switchport mode	2-690
switchport mode private-vlan	2-693
switchport port-security	2-696
switchport port-security aging	2-700
switchport private-vlan	2-702
switchport protected	2-704
switchport trunk	2-706
switchport vlan mapping	2-708
system env temperature threshold yellow	2-711
system mtu	2-712
table-map	2-715
test cable-diagnostics tdr	2-717
traceroute mac	2-719
traceroute mac ip	2-722
udld	2-724
udld port	2-726
udld reset	2-728
uni count	2-729
uni-vlan	2-731

violate-action 2-733

vlan 2-735

vlan access-map 2-738

vlan dot1q tag native 2-740

vlan filter 2-742

vmpls reconfirm (privileged EXEC) 2-744

vmpls reconfirm (global configuration) 2-745

vmpls retry 2-746

vmpls server 2-747

vrf upgrade-cli multi-af-mode 2-749

**APPENDIX A**

**Cisco ME 3400E Ethernet Access Switch  
Boot Loader Commands A-1**

arp A-2

boot A-3

cat A-5

copy A-6

delete A-7

dir A-8

flash\_init A-10

format A-11

fsck A-12

help A-13

memory A-14

mgmt\_clr A-15

mgmt\_init A-16

mgmt\_show A-17

mkdir A-18

more A-19

rename A-20

reset A-21

rmdir A-22

set A-23

type A-26

unset A-27

version A-29

**APPENDIX B****Cisco ME 3400E Ethernet Access Switch  
Debug Commands B-1**

debug backup	B-2
debug dot1x	B-3
debug etherchannel	B-4
debug ethernet service	B-5
debug interface	B-7
debug ip dhcp snooping	B-8
debug ip igmp filter	B-9
debug ip igmp max-groups	B-10
debug ip igmp snooping	B-11
debug ip sla error twamp connection	B-12
debug ip sla error twamp control reflector	B-14
debug ip sla error twamp control server	B-16
debug ip sla error twamp session	B-18
debug ip sla trace twamp connection	B-20
debug ip sla trace twamp control reflector	B-22
debug ip sla trace twamp control server	B-24
debug ip sla trace twamp session	B-26
debug ip verify source packet	B-28
debug lacp	B-29
debug mac-notification	B-30
debug matm	B-31
debug matm move update	B-32
debug monitor	B-33
debug mvrdbg	B-34
debug nvram	B-35
debug pagp	B-36
debug platform acl	B-37
debug platform backup interface	B-38
debug platform cfm	B-39
debug platform cpu-queues	B-40
debug platform dot1ad	B-42
debug platform dot1x	B-43
debug platform etherchannel	B-44
debug platform forw-tcam	B-45

debug platform ip arp inspection	<b>B-46</b>
debug platform ip dhcp	<b>B-47</b>
debug platform ip igmp snooping	<b>B-48</b>
debug platform ip multicast	<b>B-50</b>
debug platform ip source-guard	<b>B-52</b>
debug platform ip unicast	<b>B-53</b>
debug platform ipc	<b>B-55</b>
debug platform led	<b>B-56</b>
debug platform matm	<b>B-57</b>
debug platform messaging application	<b>B-58</b>
debug platform phy	<b>B-59</b>
debug platform pm	<b>B-61</b>
debug platform policer cpu uni-eni	<b>B-63</b>
debug platform port-asic	<b>B-64</b>
debug platform port-security	<b>B-65</b>
debug platform qos-acl-tcam	<b>B-66</b>
debug platform qos-manager	<b>B-67</b>
debug platform remote-commands	<b>B-68</b>
debug platform rep	<b>B-69</b>
debug platform resource-manager	<b>B-70</b>
debug platform snmp	<b>B-71</b>
debug platform span	<b>B-72</b>
debug platform supervisor-asic	<b>B-73</b>
debug platform sw-bridge	<b>B-74</b>
debug platform tcam	<b>B-75</b>
debug platform udlid	<b>B-77</b>
debug platform vlan	<b>B-78</b>
debug pm	<b>B-79</b>
debug port-security	<b>B-81</b>
debug rep	<b>B-82</b>
debug qos-manager	<b>B-83</b>
debug spanning-tree	<b>B-84</b>
debug spanning-tree bpdu	<b>B-86</b>
debug spanning-tree bpdu-opt	<b>B-87</b>
debug spanning-tree mstp	<b>B-88</b>



debug spanning-tree switch	B-90
debug sw-vlan	B-92
debug sw-vlan ifs	B-93
debug sw-vlan notification	B-94
debug udld	B-96
debug vqpc	B-98

**APPENDIX C****Cisco ME 3400E Ethernet Access Switch****Show Platform Commands C-1**

show platform acl	C-2
show platform backup interface	C-3
show platform cfm	C-4
show platform configuration	C-5
show platform dl	C-6
show platform etherchannel	C-7
show platform forward	C-8
show platform frontend-controller	C-10
show platform ip igmp snooping	C-11
show platform ip multicast	C-12
show platform ip unicast	C-13
show platform ipc trace	C-14
show platform ipv6 unicast	C-15
show platform l2pt dm	C-17
show platform layer4op	C-18
show platform mac-address-table	C-19
show platform messaging	C-20
show platform monitor	C-21
show platform mvr table	C-22
show platform pm	C-23
show platform policer cpu	C-24
show platform port-asic	C-28
show platform port-security	C-32
show platform qos	C-33
show platform resource-manager	C-36
show platform snmp counters	C-38
show platform spanning-tree synchronization	C-39

- show platform status C-40
- show platform stp-instance C-41
- show platform tcam C-42
- show platform vlan C-44
- show platform vlan mapping C-45

---

**APPENDIX D**

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

---

**INDEX**



## Preface

---

### Audience

This guide is for the networking professional using the Cisco IOS command-line interface (CLI) to manage the Cisco Metro Ethernet (ME) 3400E Series Ethernet Access switch, hereafter referred to as *the switch*. Before using this guide, you should have experience working with the Cisco IOS commands and the switch software features. You should also have experience working with the concepts and terminology of Ethernet and local area networking.

### Purpose

The switch ships with one of these software images installed:

- The metro access image includes additional features such as IEEE 802.1Q tunneling, Layer 2 protocol tunneling, dynamic ARP inspection, and IP source guard.
- The metro IP access image adds Layer 3 functionality such as IP routing support for Routing Information Protocol (RIP), Open Shortest Path First (OSPF) Protocol, Border Gateway Protocol (BGP), and Enhanced Interior Gateway Routing Protocol (EIGRP), multiple VPN routing/forwarding on customer edge (multi-VRF-CE) devices, and IP multicast routing.

This guide provides the information you need about the Layer 2 and Layer 3 commands that have been created or changed for use with the Cisco ME 3400E Ethernet Access switch. For information about the standard Cisco IOS Release 12.2 commands, see the Cisco IOS documentation set available from the Cisco.com home page by selecting **Service and Support > Technical Documents**. On the Cisco Product Documentation home page, select **Release 12.2** from the Cisco IOS Software drop-down list.

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

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

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

## Conventions

This publication uses these conventions to convey instructions and information:

Command descriptions use these conventions:

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

Interactive examples use these conventions:

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

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



### Note

---

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

---



### Caution

---

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

---

## Filtering show Command Output

The **show** commands have optional output modifiers to filter the command output.

- **| begin**—Display begins with the line that matches the *expression*.
- **| exclude**—Display excludes with the line that matches the *expression*.
- **| include**—Display includes with the line that matches the *expression*.
- *expression*—Expression in the output to use as a reference point.

Expressions are case sensitive. If you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

## Related Publications

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

[http://www.cisco.com/en/US/products/ps9637/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps9637/tsd_products_support_series_home.html)

**Note**

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

- For initial configuration information, see the “Configuring the Switch with the CLI-Based Setup Program” appendix in the hardware installation guide.
- For upgrading information, see the “Downloading Software” section in the release notes.

- *Release Notes for the Cisco ME 3400E Ethernet Access Switch*
- *Cisco ME 3400E Ethernet Access Switch Software Configuration Guide*
- *Cisco ME 3400E Ethernet Access Switch Command Reference*
- *Cisco ME 3400E, ME 3400, and ME 2400 Switch System Message Guide*
- *Cisco ME 3400E Ethernet Access Switch Hardware Installation Guide*
- *Cisco ME 3400E Switch Getting Started Guide*
- *Regulatory Compliance and Safety Information for the Cisco ME 3400E Ethernet Access Switch*
- *Cisco Small Form-Factor Pluggable Modules Installation Notes*
- *Cisco CWDM GBIC and CWDM SFP Installation Note*
- These compatibility matrix documents are available from this Cisco.com site:

[http://www.cisco.com/en/US/products/hw/modules/ps5455/products\\_device\\_support\\_tables\\_list.html](http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html)

- *Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix*
- *Cisco 100-Megabit Ethernet SFP Modules Compatibility Matrix*
- *Cisco Small Form-Factor Pluggable Modules Compatibility Matrix*
- *Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules*

## Obtaining Documentation and Submitting a Service Request

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

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

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





# CHAPTER 1

## Using the Command-Line Interface

---

The Cisco Metro Ethernet (ME) 3400E Series Ethernet Access switch is supported by Cisco IOS software. This chapter describes how to use the switch command-line interface (CLI) to configure software features.

For a complete description command descriptions, see these sections:

- For the configuration and monitoring commands that support these features, see [Chapter 2, “Cisco ME 3400E Ethernet Access Switch Cisco IOS Commands.”](#)
- For information on the boot loader commands, see [Appendix A, “Cisco ME 3400E Ethernet Access Switch Boot Loader Commands.”](#)
- For information on the **debug** commands, see [Appendix B, “Cisco ME 3400E Ethernet Access Switch Debug Commands.”](#)
- For information on the **show platform** commands, see [Appendix C, “Cisco ME 3400E Ethernet Access Switch Show Platform Commands.”](#)
- For more information on Cisco IOS Release 12.2, see the *Cisco IOS Release 12.2 Command Summary*.

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

In this document, unless otherwise specified, IP refers to IP version 4 (IPv4).

## CLI Command Modes

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

These are the main command modes for the switch:

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

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

**Table 1-1 Command Modes Summary**

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

## User EXEC Mode

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

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

```
Switch> ?
```



## Privileged EXEC Mode

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

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

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

```
Switch#
```

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

```
Switch> enable
Switch#
```

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

```
Switch# ?
```

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

## Global Configuration Mode

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

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

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

You can specify either the terminal or nonvolatile RAM (NVRAM) as the source of configuration commands.

This example shows you how to access global configuration mode:

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

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

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

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

## Interface Configuration Mode

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

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

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

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

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

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

## VLAN Configuration Mode

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

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

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

To display a comprehensive list of available commands, enter a question mark (?) at the prompt.

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

For extended-range VLANs, many characteristics are not configurable and must remain at the default setting.

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

## Line Configuration Mode

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

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

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

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

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

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





## CHAPTER 2

# Cisco ME 3400E Ethernet Access Switch Cisco IOS Commands

---

## aaa accounting dot1x

Use the **aaa accounting dot1x** global configuration command 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 **no** form of this command to disable IEEE 802.1x accounting.

```
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

<b>name</b>	Name of a server group. This is optional when you enter it after the <b>broadcast group</b> and <b>group</b> keywords.
<b>default</b>	Use the accounting methods that follow as the default list for accounting services.
<b>start-stop</b>	Send 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.
<b>broadcast</b>	Enable 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.
<b>group</b>	Specify the server group to be used for accounting services. These are valid server group names: <ul style="list-style-type: none"><li>• <b>name</b>—Name of a server group.</li><li>• <b>radius</b>—List of all RADIUS hosts.</li><li>• <b>tacacs+</b>—List of all TACACS+ hosts.</li></ul> The <b>group</b> keyword is optional when you enter it after the <b>broadcast group</b> and <b>group</b> keywords. You can enter more than optional <b>group</b> keyword.

---

## ■ aaa accounting dot1x

<b>radius</b>	(Optional) Enable RADIUS authorization.
<b>tacacs+</b>	(Optional) Enable TACACS+ accounting.

**Defaults**

AAA accounting is disabled.

**Command Modes**

Global configuration

**Command History**

Release	Modification
12.2(44)EY	This command was introduced.

**Usage Guidelines**

This command requires access to a RADIUS server.

**Note**

We recommend that you enter the **dot1x reauthentication** interface configuration command before configuring IEEE 802.1x RADIUS accounting on an interface.

**Examples**

This example shows how to configure IEEE 802.1x accounting:

```
Switch(config)# aaa accounting dot1x
Switch(config)# aaa accounting dot1x default start-stop group radius
Switch(config)#
```

**Note**

The RADIUS authentication server must be properly configured to accept and log update or watchdog packets from the AAA client.

**Related Commands**

Command	Description
<a href="#">aaa authentication dot1x</a>	Specifies one or more AAA methods for use on interfaces running IEEE 802.1x.
<a href="#">aaa-new-model</a>	Enables the AAA access control model. For syntax information, see the <b>Cisco IOS Security Command Reference, Release 12.2&gt; Authentication, Authorization, and Accounting &gt; Authentication Commands</b> .
<a href="#">dot1x reauthentication</a>	Enables or disables periodic re-authentication.
<a href="#">dot1x timeout reauth period</a>	Sets the number of seconds between re-authentication attempts.

# aaa authentication dot1x

Use the **aaa authentication dot1x** global configuration command to specify the authentication, authorization, and accounting (AAA) method to use on ports complying with IEEE 802.1x. Use the **no** form of this command to disable authentication.

```
aaa authentication dot1x {default} method1
```

```
no aaa authentication dot1x {default}
```

## Syntax Description

<b>default</b>	Use the listed authentication method that follows this argument as the default method when a user logs in.
<i>method1</i>	Enter the <b>group radius</b> 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.

## Defaults

No authentication is performed.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The *method* argument identifies the method that the authentication algorithm tries in the given sequence to validate the password provided by the client. The only method that is truly 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.

## Examples

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.

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
```

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

Related Commands	Command	Description
	<b>aaa new-model</b>	Enables the AAA access control model. For syntax information, see the <b>Cisco IOS Security Command Reference, Release 12.2 &gt; Authentication, Authorization, and Accounting &gt; Authentication Commands</b> .
	<b>show running-config</b>	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: <a href="http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html">http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html</a> Select the <b>Cisco IOS Commands Master List, Release 12.2</b> to navigate to the command.



# action

Use the **action** access-map configuration command to set the action for the VLAN access map entry. Use the **no** form of this command to set the action to the default value, which is to forward.

**action {drop | forward}**

**no action**

## Syntax Description

<b>drop</b>	Drop the packet when the specified conditions are matched.
<b>forward</b>	Forward the packet when the specified conditions are matched.

## Defaults

The default action is to forward packets.

## Command Modes

Access-map configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

You enter access-map configuration mode by using the **vlan access-map** global configuration command.

If the action is **drop**, you should define the access map, including configuring any access control list (ACL) names in match clauses, before applying the map to a VLAN, or all packets could be dropped.

In access-map configuration mode, use the **match** access-map configuration command to define the match conditions for a VLAN map. Use the **action** command to set the action that occurs when a packet matches the conditions.

The drop and forward parameters are not used in the **no** form of the command.

## Examples

This example shows how to identify and apply a VLAN access map *vmap4* to VLANs 5 and 6 that causes the VLAN to forward an IP packet if the packet matches the conditions defined in access list *a12*:

```
Switch(config)# vlan access-map vmap4
Switch(config-access-map)# match ip address a12
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan filter vmap4 vlan-list 5-6
```

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

Related Commands	Command	Description
	<b>access-list {deny   permit}</b>	Configures a standard numbered ACL. For syntax information, select <b>Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 &gt; IP Services Commands</b> .
	<b>ip access-list</b>	Creates a named access list. For syntax information, select <b>Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 &gt; IP Services Commands</b> .
	<b>mac access-list extended</b>	Creates a named MAC address access list.
	<b>match (access-map configuration)</b>	Defines the match conditions for a VLAN map.
	<b>show vlan access-map</b>	Displays the VLAN access maps created on the switch.
	<b>vlan access-map</b>	Creates a VLAN access map.

# alarm-contact

Use the **alarm-contact** global configuration command to configure triggers and severity levels for external alarms. Use the **no** form of this command to remove the configuration.

**alarm-contact** {*contact-number* {**description** *string* | **severity** {**critical** | **major** | **minor**} | **trigger** {**closed** | **open**}} | **all** {**severity** {**critical** | **major** | **minor**} | **trigger** {**closed** | **open**}}

**no alarm-contact** {*contact-number* {**description** | **severity** | **trigger**} | **all** {**severity** | **trigger**}}

<i>contact-number</i>	Configure a specific alarm contact number. The range is 1 to 4.
<b>description</b> <i>string</i>	Add a description for the alarm contact number. The description string can be up to 80 alphanumeric characters in length and is included in the system message generated when the alarm is triggered.
<b>all</b>	Configure all alarm contacts.
<b>severity</b>	Set the severity level that is set when the alarm is triggered. The severity is included in the alarm notification. Entering <b>no alarm-contact severity</b> sets the severity to minor.
<b>critical</b>	Set severity level as critical.
<b>major</b>	Set severity level as major.
<b>minor</b>	Set severity level as minor.
<b>trigger</b>	Set the state that triggers the alarm, whether the connected circuit is open or closed. Entering <b>no alarm-contact trigger</b> sets the trigger to closed.
<b>closed</b>	Specify that the alarm is triggered when the contact is closed.
<b>open</b>	Specify that the alarm is triggered when the contact is open.

## Defaults

No alarms are configured.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The **no alarm-contact** *contact-number* **description** sets the description to an empty string.

The **no alarm-contact** {*contact-number* | **all**} **severity** sets the alarm-contact severity to minor.

The **no alarm-contact** {*contact-number* | **all**} **trigger** sets the external alarm-contact trigger to closed.

**Examples**

This example shows how to configure alarm contact number 1 to report a critical alarm when the contact is open.

```
Switch(config)# alarm-contact 1 description main_lab_door
Switch(config)# alarm-contact 1 severity critical
Switch(config)# alarm-contact 1 trigger open
Dec 4 10:34:09.049: %PLATFORM_ENV-1-EXTERNAL_ALARM_CONTACT_ASSERT: Alarm asserted:
main_lab_door
```

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

```
Switch# show env alarm-contact
ALARM CONTACT 1
  Status:      asserted
  Description: main_lab_door
  Severity:    critical
  Trigger:     open
```

This example shows how to configure clear alarm contact number 1 and the show command outputs.

```
Switch(config)# no alarm-contact 1 description
Dec 4 10:39:33.621: %PLATFORM_ENV-1-EXTERNAL_ALARM_CONTACT_CLEAR: Alarm cleared:
main_lab_door Dec 4 10:39:33.621: %PLATFORM_ENV-1-EXTERNAL_ALARM_CONTACT_ASSERT: Alarm
asserted: external alarm contact 1

Switch(config)# no alarm-contact 1 severity
Dec 4 10:39:46.774: %PLATFORM_ENV-1-EXTERNAL_ALARM_CONTACT_CLEAR: Alarm cleared: external
alarm contact 1 Dec 4 10:39:46.774: %PLATFORM_ENV-1-EXTERNAL_ALARM_CONTACT_ASSERT: Alarm
asserted: external alarm contact 1

Switch(config)# no alarm-contact 1 trigger open
Dec 4 10:39:56.547: %PLATFORM_ENV-1-EXTERNAL_ALARM_CONTACT_CLEAR: Alarm cleared: external
alarm contact 1

Switch(config)# end
Switch# show env alarm-contact
ALARM CONTACT 1
  Status:      not asserted
  Description: external alarm contact 1
  Severity:    minor
  Trigger:     closed
Switch# show hard led
SWITCH: 1
SYSTEM: GREEN
MGMT: GREEN
ALARM 1: BLACK
ALARM 2: BLACK
ALARM 3: BLACK
ALARM 4: BLACK
```

**Related Commands**

Command	Description
<b>show env alarm-contact</b>	Displays the alarm setting and status for the switch.

# archive download-sw

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

```
archive download-sw {/force-reload | /imageonly | /leave-old-sw | /no-set-boot |
/no-version-check | /overwrite | /reload | /safe} source-url
```

Syntax	Description
<b>/force-reload</b>	Unconditionally force a system reload after successfully downloading the software image.
<b>/imageonly</b>	Download only the software image but not the HTML files associated with the embedded device manager. The HTML files for the existing version are deleted only if the existing version is being overwritten or removed.
<b>/leave-old-sw</b>	Keep the old software version after a successful download.
<b>/no-set-boot</b>	Do not alter the setting of the BOOT environment variable to point to the new software image after it is successfully downloaded.
<b>/no-version-check</b>	Download the software image without checking to prevent installing an incompatible image.
<b>/overwrite</b>	Overwrite the software image in flash memory with the downloaded one.
<b>/reload</b>	Reload the system after successfully downloading the image unless the configuration has been changed and not been saved.
<b>/safe</b>	Keep the current software image; do not delete it to make room for the new software image before the new image is downloaded. The current image is deleted after the download.
<i>source-url</i>	<p>The source URL alias for a local or network file system. These options are supported:</p> <ul style="list-style-type: none"> <li>The syntax for the local flash file system: <b>flash:</b></li> <li>The syntax for the FTP: <b>ftp:[[/username[:password]@location]/directory]/image-name.tar</b></li> <li>The syntax for an HTTP server: <b>http://[[username:password]@]{hostname   host-ip}/[directory]/image-name.tar</b></li> <li>The syntax for a secure HTTP server: <b>https://[[username:password]@]{hostname   host-ip}/[directory]/image-name.tar</b></li> <li>The syntax for the Remote Copy Protocol (RCP): <b>rcp:[[/username@location]/directory]/image-name.tar</b></li> <li>The syntax for the TFTP: <b>tftp:[[/location]/directory]/image-name.tar</b></li> </ul> <p>The <i>image-name.tar</i> is the software image to download and install on the switch.</p>

**Defaults**

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

Both the software image and HTML files are downloaded.

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

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

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

Compatibility of the version on the image to be downloaded is checked.

**Command Modes**

Privileged EXEC

**Command History**

Release	Modification
12.2(44)EY	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 leaving the software in place prevents the new image from fitting in flash memory due to space constraints, an error results.

If you used the **/leave-old-sw** option and did not overwrite the old image when you downloaded the new one, you can remove the old image by using the **delete** privileged EXEC command. For more information, see the “[delete](#)” section on page 2-80.

**Note**

Use the **/no-version-check** option with care. This option allows an image to be downloaded without first confirming that it is not incompatible with the switch.

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

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

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

**Examples**

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

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

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

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

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

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

**Related Commands**

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

## archive tar

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

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

### Syntax Description

**/create** *destination-url*  
**flash:**/*file-url*

Create a new tar file on the local or network file system.

For *destination-url*, specify 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 syntax for the local flash filesystem:  
**flash:**
- The syntax for the FTP:  
**ftp:**[[//*username[:password]*@*location*]/*directory*]/*tar-filename.tar*
- The syntax for the Remote Copy Protocol (RCP) is:  
**rcp:**[[//*username*@*location*]/*directory*]/*tar-filename.tar*
- The syntax for the TFTP:  
**tftp:**[[//*location*]/*directory*]/*tar-filename.tar*

The *tar-filename.tar* is the tar file to be created.

For **flash:**/*file-url*, specify the location on the local flash file system from which the new tar file is created.

An optional list of files or directories within the source directory can be specified to write to the new tar file. If none are specified, all files and directories at this level are written to the newly created tar file.

**/table** *source-url*

Display the contents of an existing tar file to the screen.

For *source-url*, specify the source URL alias for the local or network file system. These options are supported:

- The syntax for the local flash file system:  
**flash:**
- The syntax for the FTP:  
**ftp:**[[//*username[:password]*@*location*]/*directory*]/*tar-filename.tar*
- The syntax for the RCP:  
**rcp:**[[//*username*@*location*]/*directory*]/*tar-filename.tar*
- The syntax for the TFTP:  
**tftp:**[[//*location*]/*directory*]/*tar-filename.tar*

The *tar-filename.tar* is the tar file to display.



---

<b>/xtract</b> <i>source-url</i> <b>flash:</b> <i>/file-url [dir/file...]</i>	<p>Extract files from a tar file to the local file system.</p> <p>For <i>source-url</i>, specify the source URL alias for the local file system. These options are supported:</p> <ul style="list-style-type: none"> <li>• The syntax for the local flash file system: <b>flash:</b></li> <li>• The syntax for the FTP: <b>ftp:</b><i>[[//username[:password]@location]/directory]/tar-filename.tar</i></li> <li>• The syntax for the RCP: <b>rcp:</b><i>[[//username@location]/directory]/tar-filename.tar</i></li> <li>• The syntax for the TFTP: <b>tftp:</b><i>[[//location]/directory]/tar-filename.tar</i></li> </ul> <p>The <i>tar-filename.tar</i> is the tar file from which to extract.</p> <p>For <b>flash:</b><i>/file-url [dir/file...]</i>, specify the location on the local flash file system into which the tar file is extracted. Use the <i>dir/file...</i> 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.</p>
--	--

---



---

**Defaults** None

---

**Command Modes** Privileged EXEC

---

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

---



---

**Usage Guidelines** Filenames and directory names are case sensitive.  
Image names are case sensitive.

---

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

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

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

```
Switch# archive tar /table flash:image_name-mz.122-release.tar
info (219 bytes)
image_name-mz.122-release/(directory)
image_name-mz.122-release(610856 bytes)
image_name-mz.122-release/info (219 bytes)
info.ver (219 bytes)
```

This example shows how to display only the *html* directory and its contents:

```
Switch# archive tar /table flash:image_name-mz.122-release.tar
image_name-mz.122-release/html
image_name-mz.122-release/html/ (directory)
image_name-mz.122-release/html/const.htm (556 bytes)
image_name-mz.122-release/html/xhome.htm (9373 bytes)
image_name-mz.122-release/html/menu.css (1654 bytes)
<output truncated>
```

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

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

#### Related Commands

Command	Description
<a href="#">Command History</a>	Downloads a new image from a TFTP server to the switch.
<a href="#">archive upload-sw</a>	Uploads an existing image on the switch to a server.

# archive upload-sw

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

**archive upload-sw** [/version *version\_string*] **destination-url**

Syntax Description	
<i>/version version_string</i>	(Optional) Specify the specific version string of the image to be uploaded.
<i>destination-url</i>	<p>The destination URL alias for a local or network file system. These options are supported:</p> <ul style="list-style-type: none"> <li>The syntax for the local flash file system: <b>flash:</b></li> <li>The syntax for the FTP: <b>ftp:[[/username[:password]@location]/directory]/image-name.tar</b></li> <li>The syntax for the Remote Copy Protocol (RCP): <b>rcp:[[/username@location]/directory]/image-name.tar</b></li> <li>The syntax for the TFTP: <b>tftp:[[/location]/directory]/image-name.tar</b></li> </ul> <p>The <i>image-name.tar</i> is the name of software image to be stored on the server.</p>

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

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

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

Image names are case sensitive.

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

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

■ archive upload-sw

Related Commands	Command	Description
	<a href="#">Command History</a>	Downloads a new image to the switch.
	<a href="#">archive tar</a>	Creates a tar file, lists the files in a tar file, or extracts the files from a tar file.

# arp access-list

Use the **arp access-list** global configuration command to define an Address Resolution Protocol (ARP) access control list (ACL) or to add clauses to the end of a previously defined list. Use the **no** form of this command to delete the specified ARP access list.

**arp access-list** *acl-name*

**no arp access-list** *acl-name*

<b>Syntax Description</b>	<i>acl-name</i>	Name of the ACL.
<b>Defaults</b>	No ARP access lists are defined.	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

**Usage Guidelines** After entering the **arp access-list** command, you enter ARP access-list configuration mode, and these configuration commands are available:

- **default:** returns a command to its default setting.
- **deny:** specifies packets to reject. For more information, see the [“deny \(ARP access-list configuration\)” section on page 2-81](#).
- **exit:** exits ARP access-list configuration mode.
- **no:** negates a command or returns to the default settings.
- **permit:** specifies packets to forward. For more information, see the [“permit \(ARP access-list configuration\)” section on page 2-322](#).

Use the **permit** and **deny** access-list configuration commands to forward and to drop ARP packets based on the specified matching criteria.

When the ARP ACL is defined, you can apply it to a VLAN by using the **ip arp inspection filter vlan** global configuration command. ARP packets containing only IP-to-MAC address bindings are compared to the ACL. All other types of packets are bridged in the ingress VLAN without validation. If the ACL permits a packet, the switch forwards it. If the ACL denies a packet because of an explicit deny statement, the switch drops the packet. If the ACL denies a packet because of an implicit deny statement, the switch compares the packet to the list of DHCP bindings (unless the ACL is *static*, which means that packets are not compared to the bindings).

**Examples**

This example shows how to define an ARP access list and to permit both ARP requests and ARP responses from a host with an IP address of 1.1.1.1 and a MAC address of 0000.0000.abcd:

```
Switch(config)# arp access-list static-hosts
Switch(config-arp-nacl)# permit ip host 1.1.1.1 mac host 0000.0000.abcd
Switch(config-arp-nacl)# end
```

You can verify your settings by entering the **show arp access-list** privileged EXEC command.

**Related Commands**

Command	Description
<b>deny (ARP access-list configuration)</b>	Denies an ARP packet based on matches compared against the DHCP bindings.
<b>ip arp inspection filter vlan</b>	Permits ARP requests and responses from a host configured with a static IP address.
<b>permit (ARP access-list configuration)</b>	Permits an ARP packet based on matches compared against the DHCP bindings.
<b>show arp access-list</b>	Displays detailed information about ARP access lists.

# bandwidth

Use the **bandwidth** policy-map class configuration command to configure class-based weighted fair queuing (CBWFQ) by setting the output bandwidth for a policy-map class. Use the **no** form of this command to remove the bandwidth setting for the class.

**bandwidth** {*rate* | **percent** *value* | **remaining percent** *value*}

**no bandwidth** [*rate* | **percent** *value* | **remaining percent** *value*]

## Syntax Description

<i>rate</i>	Set the bandwidth rate for the class in kilobits per second (kbps). The range is from 64 to 1000000.
<b>percent</b> <i>value</i>	Set the bandwidth for the class as a percent of the total bandwidth. The range is from 1 to 100 percent.
<b>remaining percent</b> <i>value</i>	Set the bandwidth for the class as a percent of the remaining bandwidth. The range is from 1 to 100 percent.

## Defaults

No bandwidth is defined.

## Command Modes

Policy-map class configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

You use the **bandwidth** policy-map class command to control output traffic. The **bandwidth** command specifies the bandwidth for traffic in that class. CBWFQ derives the weight for packets belonging to the class from the bandwidth allocated to the class and uses the weight to ensure that the queue for that class is serviced fairly. Bandwidth settings are not supported in input policy maps.

When you configure bandwidth for a class of traffic as an absolute rate (kbps) or a percentage of bandwidth (**percent** *value*), it represents the minimum bandwidth guarantee or committed information rate (CIR) for that traffic class. This means that the traffic class gets at least the bandwidth specified in the command, but is not limited to that bandwidth. Any excess bandwidth on the port is allocated to each class in the same ratio as the configured CIR rates.

When you enter the **bandwidth remaining percent** command, hard bandwidths are not guaranteed, and only relative bandwidths are assured. Class bandwidths are always proportional to the specified bandwidth percentages configured for the port.

When you configure bandwidth in an output policy, you must specify the same units in each bandwidth configuration; that is, all absolute values (rates) or percentages.

The total rate of the minimum bandwidth guarantees for each queue of the policy cannot exceed the total speed for the interface. If the **percent** keyword is used, the sum of the class bandwidth percentages cannot exceed 100 percent.

Using the **queue-limit** command to modify the default queue limit is especially important on higher-speed interfaces so that they meet the minimum bandwidth guarantees required by the interface.

You cannot use the **bandwidth** policy-map class configuration command to configure CBWFQ and the **shape average** command to configure class-based shaping for the same class in a policy map.

You cannot configure bandwidth in a class that includes priority queuing (configured with the **priority** policy-map class configuration command).

## Examples

This example shows how to set the precedence of output queues by setting bandwidth in kilobits per second. The classes *outclass1*, *outclass2*, and *outclass3* get a minimum of 50000, 20000, and 10000 kbps. The class **class-default** at a minimum gets the remaining bandwidth.

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# bandwidth 50000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth 20000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth 10000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

This example shows how to set the precedence of output queues by allocating percentages of the total available bandwidth to each traffic class. The classes *outclass1*, *outclass2*, and *outclass3* get a minimum of 50, 20, and 10 percent. The class **class-default** at a minimum gets 20 percent.

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```



This example shows how to set *outclass1* as a priority queue, with *outclass2*, and *outclass3* getting 50 and 20 percent, respectively, of the bandwidth remaining after the priority queue is serviced. The class **class-default** gets the remaining 30 percent with no guarantees.

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

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

#### Related Commands

Command	Description
<a href="#">class</a>	Defines a traffic classification match criteria for the specified class-map name.
<a href="#">policy-map</a>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
<a href="#">show policy-map</a>	Displays quality of service (QoS) policy maps.

# boot buffersize

Use the **boot buffersize** global configuration command to configure the NVRAM size. Use the **no** form of this command to return to the default.

**boot buffersize** *size*

**no boot buffersize**

Syntax Description	<i>size</i>	The NVRAM buffer size in KB. The valid range is from 4096 to 1048576.
--------------------	-------------	--

Defaults	The default NVRAM buffer size is 512 KB.
----------	--

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	12.2(55)SE	This command was introduced.

Usage Guidelines	The default NVRAM buffer size is 512 KB. In some cases, the configuration file might be too large to save to NVRAM. You can configure the size of the NVRAM buffer to support larger configuration files. After you configure the NVRAM buffer size, reload the switch.
------------------	---

Examples	This example shows how to configure the NVRAM buffer size: <pre>Switch(config)# <b>boot buffersize 524288</b> Switch(config)# <b>end</b></pre>
----------	---

Related Commands	Command	Description
	<b>show boot</b>	Displays the settings of the boot environment variables.

# boot config-file

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

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

**no boot config-file**

Syntax Description	flash:	<i>file-url</i>	The path (directory) and name of the configuration file.
--------------------	--------	-----------------	--

Defaults	The default configuration file is flash:config.text.
----------	--

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

Usage Guidelines	<p>Filenames and directory names are case sensitive.</p> <p>This command changes the setting of the CONFIG_FILE environment variable. For more information, see <a href="#">Appendix A, “Cisco ME 3400E Ethernet Access Switch Boot Loader Commands.”</a></p>
------------------	---

Related Commands	Command	Description
	<a href="#">show boot</a>	Displays the settings of the boot environment variables.

# boot enable-break

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

**boot enable-break**

**no boot enable-break**

**Syntax Description** This command has no arguments or keywords.

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

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** When you enter this command, you can interrupt the automatic boot process by pressing the break key on the console after the flash file system is initialized. The break key is different for each operating system:

- On a SUN work station running UNIX, Ctrl-C is the break key.
- On a PC running Windows 2000, Ctrl-Break is the break key.

This command changes the setting of the ENABLE\_BREAK environment variable. For more information, see [Appendix A, "Cisco ME 3400E Ethernet Access Switch Boot Loader Commands."](#)

Related Commands	Command	Description
	<a href="#">show boot</a>	Displays the settings of the boot environment variables.

# boot helper

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

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

**no boot helper**

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

**Defaults** No helper files are loaded.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** This variable is used only for internal development and testing.  
 Filenames and directory names are case sensitive.  
 This command changes the setting of the HELPER environment variable. For more information, see [Appendix A, “Cisco ME 3400E Ethernet Access Switch Boot Loader Commands.”](#)

Related Commands	Command	Description
	<a href="#">show boot</a>	Displays the settings of the boot environment variables.

## boot helper-config-file

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

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

**no boot helper-config file**

Syntax	Description
<i>filesystem:</i>	Alias for a flash file system. Use <b>flash:</b> for the system board flash device.
<i>/file-url</i>	The path (directory) and helper configuration file to load.

**Defaults** No helper configuration file is specified.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** This variable is used only for internal development and testing.

Filenames and directory names are case sensitive.

This command changes the setting of the HELPER\_CONFIG\_FILE environment variable. For more information, see [Appendix A, “Cisco ME 3400E Ethernet Access Switch Boot Loader Commands.”](#)

Related Commands	Command	Description
	<a href="#">show boot</a>	Displays the settings of the boot environment variables.

# boot manual

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

**boot manual**

**no boot manual**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Manual booting is disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

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

This command changes the setting of the MANUAL\_BOOT environment variable. For more information, see [Appendix A, “Cisco ME 3400E Ethernet Access Switch Boot Loader Commands.”](#)

Related Commands	Command	Description
	<a href="#">show boot</a>	Displays the settings of the boot environment variables.

## boot private-config-file

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

**boot private-config-file** *filename*

**no boot private-config-file**

### Syntax Description

<i>filename</i>	The name of the private configuration file.
-----------------	---

### Defaults

The default configuration file is *private-config*.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

Filenames are case sensitive.

### Examples

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

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

### Related Commands

Command	Description
<a href="#">show boot</a>	Displays the settings of the boot environment variables.



# boot system

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

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

**no boot system**

## Syntax Description

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

## Defaults

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

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

Filenames and directory names are case sensitive.

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

This command changes the setting of the BOOT environment variable. For more information, see [Appendix A, “Cisco ME 3400E Ethernet Access Switch Boot Loader Commands.”](#)

## Related Commands

Command	Description
<a href="#">show boot</a>	Displays the settings of the boot environment variables.

# channel-group

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

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

```
no channel-group
```

PAGP modes:

```
channel-group channel-group-number mode { auto [non-silent] | { desirable [non-silent] }
```

LACP modes:

```
channel-group channel-group-number mode { active | passive }
```

On mode:

```
channel-group channel-group-number mode on
```



## Note

Link Aggregation Control Protocol (LACP) and Port Aggregation Protocol (PAgP) are available only on network node interfaces (NNIs) or enhanced network interfaces (ENIs). The **active**, **auto**, **desirable**, and **passive** keywords are not visible on user network interfaces (UNIs).

## Syntax Description

<i>channel-group-number</i>	Specify the channel group number. The range is 1 to 48.
<b>mode</b>	Specify the EtherChannel mode.
<b>active</b>	Unconditionally enable LACP  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.
<b>auto</b>	Enable the PAgP only if a PAgP device is detected.  Auto mode places a port into a passive negotiating state in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation. A channel is formed only with another port group in desirable mode. When <b>auto</b> is enabled, silent operation is the default.
<b>desirable</b>	Unconditionally enable PAgP.  Desirable mode places a port into an active negotiating state in which the port starts negotiations with other ports by sending PAgP packets. A channel is formed with another port group in either the desirable or auto mode. When <b>desirable</b> is enabled, silent operation is the default.
<b>non-silent</b>	(Optional) Use in PAgP mode with the <b>auto</b> or <b>desirable</b> keyword when traffic is expected from the other device.

<b>on</b>	Enable <b>on</b> mode.  In <b>on</b> mode, a usable EtherChannel exists only when both connected port groups are in the <b>on</b> mode.
<b>passive</b>	Enable LACP only if a LACP device is detected.  Passive mode places a port into a negotiating state in which the port responds to LACP packets it receives but does not initiate LACP packet negotiation. A channel is formed only with another port group in active mode.

**Defaults**

No channel groups are assigned.  
No mode is configured.

**Command Modes**

Interface configuration

**Command History**

Release	Modification
12.2(44)EY	This command was introduced.

**Usage Guidelines**

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

If the port is a UNI or an ENI, you must use the **no shutdown** interface configuration command to enable it before using the **channel-group** command. UNIs and ENIs are disabled by default. NNIs are enabled by default.

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

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.

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

If you do not specify **non-silent** with the **auto** or **desirable** mode, silent is assumed. The silent mode is used when the switch is connected to a device that is not PAGP-capable and seldom, if ever, sends packets. A example of a silent partner is a file server or a packet analyzer that is not generating traffic.

In this case, running PAgP on a physical port prevents that port from ever becoming operational. However, it allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission. Both ends of the link cannot be set to silent.

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

**Caution**

You should exercise care when setting the mode to **on** (manual configuration). All ports configured in the **on** mode are bundled in the same group and are forced to have similar characteristics. If the group is misconfigured, packet loss or spanning-tree loops might occur.

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

**Note**

PAgP and LACP are available only on NNIs and ENIs.

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 on an EtherChannel port, an error message appears, and IEEE 802.1x is not enabled.

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

**Examples**

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

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

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

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

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

Related Commands	Command	Description
	<a href="#">channel-protocol</a>	Restricts the protocol used on a port to manage channeling.
	<a href="#">interface port-channel</a>	Accesses or creates the port channel.
	<a href="#">show etherchannel</a>	Displays EtherChannel information for a channel.
	<a href="#">show lacp</a>	Displays LACP channel-group information.
	<a href="#">show pagp</a>	Displays PAGP channel-group information.
	<a href="#">show running-config</a>	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: <a href="http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html">http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html</a> Select the <b>Cisco IOS Commands Master List, Release 12.2</b> to navigate to the command.

# channel-protocol

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

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

**no channel-protocol**

## Syntax Description

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

## Defaults

No protocol is assigned to the EtherChannel.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

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



### Note

PAgP and LACP are available only on network node interfaces (NNIs) and enhanced network interfaces (ENIs).

If the port is a user network interface (UNI) or an ENI, you must use the **no shutdown** interface configuration command to enable it before using the **channel-protocol** command. UNIs and ENIs are disabled by default. NNIs are enabled by default.

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

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

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

## Examples

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

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

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

Related Commands	Command	Description
	<a href="#">channel-group</a>	Assigns an Ethernet port to an EtherChannel group.
	<a href="#">show etherchannel protocol</a>	Displays protocol information the EtherChannel.

# class

Use the **class** policy-map configuration command to specify the name of the class whose policy you want to create or to change or to specify the system default class before you configure a policy and to enter policy-map class configuration mode. Use the **no** form of this command to remove the class from a policy map.

```
class {class-map-name| class-default}
```

```
no class {class-map-name| class-default}
```

## Syntax Description

<i>class-map-name</i>	Name of a class map created by using the <b>class-map</b> global configuration command.
<b>class-default</b>	The system default class. This class matches all unclassified traffic. You cannot create or delete the default class.

## Defaults

No policy map classes are defined.

## Command Modes

Policy-map configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

Before using the **class** *class-map-name* command in policy-map configuration mode, you must create the class by using the **class-map** *class-map-name* global configuration command. The class **class-default** is the class to which traffic is directed if that traffic does not match any of the match criteria in the configured class maps.

Use the **policy-map** global configuration command to identify the policy map and to 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.

An input policy map can have a maximum of 64 classes, plus **class-default**.

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, and these configuration commands are available:

- **bandwidth**: specifies the bandwidth allocated for a class belonging to a policy map. For more information, see the **bandwidth** command.
- **exit**: exits policy-map class configuration mode and returns to policy-map configuration mode.
- **no**: returns a command to its default setting.



- **police**: defines an individual 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 the **police** and **police aggregate (policy-map class configuration)** policy-map class commands.
- **priority**: sets the strict scheduling priority for this class or, when used with the **police** keyword, sets priority with police. For more information, see the **priority** policy-map class command.
- **queue-limit**: sets the queue maximum threshold for Weighted Tail Drop (WTD). For more information, see the **queue-limit** command.
- **service-policy**: configures a QoS service policy to attach to a parent policy map for an input or output policy. For more information, see the **service-policy (policy-map class configuration)** command.
- **set**: specifies a value to be assigned to the classified traffic. For more information, see the **set** commands.
- **shape average**: specifies the average traffic shaping rate. For more information, see the **shape average** command.

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 create a policy map called *policy1*, define a class *class1*, and enter policy-map class configuration mode to set a criterion for the class.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# exit
```

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

### Related Commands

Command	Description
<b>class-map</b>	Creates a class map to be used for matching packets to the class whose name you specify.
<b>policy-map</b>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
<b>show policy-map</b>	Displays QoS policy maps.
<b>show policy-map interface</b> [ <i>interface-id</i> ]	Displays policy maps configured on the specified interface or on all interfaces.

# class-map

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

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

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

## Syntax Description

<b>match-all</b>	(Optional) Perform a logical-AND of all matching statements under this class map. Packets must meet all of the match criteria.
<b>match-any</b>	(Optional) Perform a logical-OR of the matching statements under this class map. Packets must meet one or more of the match criteria.
<i>class-map-name</i>	Name of the class map.

## Defaults

No class maps are defined.

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

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

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

The switch supports a maximum of 1024 unique class maps.

You use the **class-map** command and class-map configuration mode to define packet classification as part of a globally named service policy applied on a per-port basis. When you configure a class map, you can use one or more **match** commands to specify match criteria. Packets arriving at either the input or output interface (determined by how you configure the **service-policy** interface configuration command) are checked against the class-map match criteria to determine if the packet belongs to that class.

A **match-all** class map means that the packet must match all entries and can have no other match statements.

After you are in class-map configuration mode, these configuration commands are available:

- **description**: describes the class map (up to 200 characters). The **show class-map** privileged EXEC command displays the description and the name of the class map.
- **exit**: exits QoS class-map configuration mode.

- **match**: configures classification criteria. For more information, see the **match** class-map configuration commands.
- **no**: removes a match statement from a class map.

### Examples

This example shows how to configure the class map called *class1*. By default, the class map is **match-all** and therefore can contain no other match criteria.

```
Switch(config)# class-map class1
Switch(config-cmap)# exit
```

This example shows how to configure a match-any class map with one match criterion, which is an access list called *103*. This class map (matching an ACL) is supported only in an input policy map.

```
Switch(config)# class-map class2
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# exit
```

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

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

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

### Related Commands

Command	Description
<b>class</b>	Defines a traffic classification match criteria for the specified class-map name.
<b>match access-group</b>	Configures the match criteria for a class map on the basis of the specified access control list (ACL)
<b>match cos</b>	Configures the match criteria for a class map on the basis of the Layer 2 class of service (CoS) marking,
<b>match ip dscp</b>	Configures the match criteria for a class map on the basis of a specific IPv4 Differentiated Service Code Point (DSCP) value.
<b>match ip precedence</b>	Configures the match criteria for a class map on the basis of IPv4 precedence values.
<b>match qos-group</b>	Configures the match criteria for a class map on the basis of a specific quality of service (QoS) group value.
<b>match vlan</b>	Configures the match criteria for a class map in the parent policy of a hierarchical policy map based on a VLAN ID or range of VLAN IDs.
<b>policy-map</b>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
<b>show class-map</b>	Displays QoS class maps.

# clear ip arp inspection log

Use the **clear ip arp inspection log** privileged EXEC command to clear the dynamic Address Resolution Protocol (ARP) inspection log buffer.

## clear ip arp inspection log

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default is defined.

**Command Modes** Privileged EXEC

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Examples

This example shows how to clear the contents of the log buffer:

```
Switch# clear ip arp inspection log
```

You can verify that the log was cleared by entering the **show ip arp inspection log** privileged command.

### Related Commands

Command	Description
<a href="#">arp access-list</a>	Defines an ARP access control list (ACL).
<a href="#">ip arp inspection log-buffer</a>	Configures the dynamic ARP inspection logging buffer.
<a href="#">ip arp inspection vlan logging</a>	Controls the type of packets that are logged per VLAN.
<a href="#">show ip arp inspection log</a>	Displays the configuration and contents of the dynamic ARP inspection log buffer.

# clear ip arp inspection statistics

Use the **clear ip arp inspection statistics** privileged EXEC command to clear the dynamic Address Resolution Protocol (ARP) inspection statistics.

**clear ip arp inspection statistics** [**vlan** *vlan-range*]

<b>Syntax Description</b>	<b>vlan</b> <i>vlan-range</i>	(Optional) Clear statistics for the specified VLAN or VLANs. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
---------------------------	-------------------------------	--

<b>Defaults</b>	No default is defined.
-----------------	------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

<b>Examples</b>	This example shows how to clear the statistics for VLAN 1:
-----------------	--

```
Switch# clear ip arp inspection statistics vlan 1
```

You can verify that the statistics were deleted by entering the **show ip arp inspection statistics vlan 1** privileged EXEC command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show ip arp inspection statistics</a>	Displays statistics for forwarded, dropped, MAC validation failure, and IP validation failure packets for all VLANs or the specified VLAN.

# clear ip dhcp snooping

Use the **clear ip dhcp snooping** privileged EXEC command to clear the DHCP binding database agent statistics or the DHCP snooping statistics counters.

**clear ip dhcp snooping** { **binding** [\* | *ip-address* | **interface** *interface-id* | **vlan** *vlan-id*] | **database statistics** | **statistics** }

## Syntax Description

<b>binding</b>	Clear the DHCP snooping binding database.
*	Clear all automatic bindings.
<i>ip-address</i>	Clear the binding entry IP address.
<b>interface</b> <i>interface-id</i>	Clear the binding input interface.
<b>vlan</b> <i>vlan-id</i>	Clear the binding entry VLAN.
<b>database statistics</b>	Clear the DHCP snooping binding database agent statistics.
<b>database statistics</b>	Clear the DHCP snooping binding database agent statistics.
<b>statistics</b>	Clear the DHCP snooping statistics counter.

## Defaults

No default is defined.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

When you enter the **clear ip dhcp snooping database statistics** command, the switch does not update the entries in the binding database and in the binding file before clearing the statistics.

## Examples

This example shows how to clear the DHCP snooping binding database agent statistics:

```
Switch# clear ip dhcp snooping database statistics
```

You can verify that the statistics were cleared by entering the **show ip dhcp snooping database** privileged EXEC command.

This example shows how to clear the DHCP snooping statistics counters:

```
Switch# clear ip dhcp snooping statistics
```

You can verify that the statistics were cleared by entering the **show ip dhcp snooping statistics** user EXEC command.

Related Commands	Command	Description
	<a href="#">ip dhcp snooping</a>	Enables DHCP snooping on a VLAN.
	<a href="#">ip dhcp snooping database</a>	Configures the DHCP snooping binding database agent or the binding file.
	<a href="#">show ip dhcp snooping binding</a>	Displays the status of DHCP snooping database agent.
	<a href="#">show ip dhcp snooping database</a>	Displays the DHCP snooping binding database agent statistics.
	<a href="#">show ip dhcp snooping statistics</a>	Displays the DHCP snooping statistics.

# clear ipc

Use the **clear ipc** privileged EXEC command to clear Interprocess Communications Protocol (IPC) statistics.

**clear ipc {queue-statistics | statistics}**

## Syntax Description

<b>queue-statistics</b>	Clear the IPC queue statistics.
<b>statistics</b>	Clear the IPC statistics.

## Defaults

No default is defined.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

You can clear all statistics by using the **clear ipc statistics** command, or you can clear only the queue statistics by using the **clear ipc queue-statistics** command.

## Examples

This example shows how to clear all statistics:

```
Switch# clear ipc statistics
```

This example shows how to clear only the queue statistics:

```
Switch# clear ipc queue-statistics
```

You can verify that the statistics were deleted by entering the **show ipc rpc** or the **show ipc session** privileged EXEC command.

## Related Commands

Command	Description
<b>show ipc {rpc   session}</b>	Displays the IPC multicast routing statistics.



# clear ipv6 dhcp conflict

Use the **clear ipv6 dhcp conflict** privileged EXEC command to clear an address conflict from the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server database.

```
clear ipv6 dhcp conflict { * | IPv6-address }
```



## Note

This command is available only if the switch is running the metro IP access image and you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

## Syntax Description

*	Clear all address conflicts.
IPv6-address	Clear the host IPv6 address that contains the conflicting address.

## Defaults

No default is defined.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(50)SE	This command was introduced.

## Usage Guidelines

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6 { default | routing | vlan }** global configuration command, and reload the switch.

When you configure the DHCPv6 server to detect conflicts, it uses ping. The client uses neighbor discovery to detect clients and reports to the server through a DECLINE message. If an address conflict is detected, the address is removed from the pool and is not assigned until the administrator removes the address from the conflict list.

If you use the asterisk (\*) character as the address parameter, DHCP clears all conflicts.

## Examples

This example shows how to clear all address conflicts from the DHCPv6 server database:

```
Switch# clear ipv6 dhcp conflict *
```

## Related Commands

Command	Description
<a href="#">show ipv6 dhcp conflict</a>	Displays address conflicts found by a DHCPv6 server, or reported through a DECLINE message from a client.

## clear l2protocol-tunnel counters

Use the **clear l2protocol-tunnel counters** privileged EXEC command to clear the protocol counters in protocol tunnel ports.

**clear l2protocol-tunnel counters** [*interface-id*]

This command is supported only when the switch is running the metro IP access or metro access image.

<b>Syntax Description</b>	<i>interface-id</i>	(Optional) Specify interface (physical interface or port channel) for which protocol counters are to be cleared.
---------------------------	---------------------	--

<b>Defaults</b>	No default is defined.
-----------------	------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

<b>Usage Guidelines</b>	Use this command to clear protocol tunnel counters on the switch or on the specified interface.
-------------------------	---

**Examples** This example shows how to clear Layer 2 protocol tunnel counters on an interface:

```
Switch# clear l2protocol-tunnel counters gigabitethernet0/2
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show l2protocol-tunnel</a>	Displays information about ports configured for Layer 2 protocol tunneling.

# clear lacp

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

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



## Note

LACP is available only on network node interfaces (NNIs) and enhanced network interfaces (ENIs).

## Syntax Description

<i>channel-group-number</i>	(Optional) Channel group number. The range is 1 to 48.
<b>counters</b>	Clear traffic counters.

## Defaults

No default is defined.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

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

## Examples

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

```
Switch# clear lacp counters
```

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

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

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

## Related Commands

Command	Description
<a href="#">show lacp</a>	Displays LACP channel-group information.

# clear logging onboard

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

**clear logging onboard** [**module** {*slot-number* | **all**}]

## Syntax Description

<b>module</b>	(Optional) The slot number is always 1 and is not relevant for the ME-3400E.
{ <i>slot-number</i>   <b>all</b> }	Entering <b>clear logging onboard module 1</b> or <b>clear logging onboard all</b> has the same result as entering <b>clear logging onboard</b> .

## Defaults

No default is defined.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

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

## Examples

These examples show how to clear all the OBFL information except for the uptime and CLI-command information:

```
Switch# clear logging onboard
Clear logging onboard buffer [confirm]
PID: ME-3400E-24TS-M , VID: 03 , SN: FOC1225U4CY
```

```
Switch# clear logging onboard module all
Clear logging onboard buffer [confirm]
PID: ME-3400E-24TS-M , VID: 03 , SN: FOC1225U4CY
```

You can verify that the information was cleared by entering the **show logging onboard onboard** privileged EXEC command.

## Related Commands

Command	Description
<a href="#">hw-module module logging onboard</a>	Enables OBFL.
<a href="#">show logging onboard</a>	Displays OBFL information.

# clear mac address-table

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

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

Syntax Description		
<b>dynamic</b>		Delete all dynamic MAC addresses.
<b>dynamic address</b> <i>mac-addr</i>		(Optional) Delete the specified dynamic MAC address.
<b>dynamic interface</b> <i>interface-id</i>		(Optional) Delete all dynamic MAC addresses on the specified physical port or port channel.
<b>dynamic vlan</b> <i>vlan-id</i>		(Optional) Delete all dynamic MAC addresses for the specified VLAN. The range is 1 to 4096.
<b>notification</b>		Clear the notifications in the history table and reset the counters.

**Defaults** No default is defined.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

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

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

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

Related Commands	Command	Description
	<a href="#">mac address-table notification</a>	Enables the MAC address notification feature.
	<a href="#">show mac address-table</a>	Displays the MAC address table static and dynamic entries.
	<a href="#">show mac address-table notification</a>	Displays the MAC address notification settings for all interfaces or the specified interface.
	<a href="#">snmp trap mac-notification change</a>	Enables the Simple Network Management Protocol (SNMP) MAC address notification trap on a specific interface.

# clear mac address-table move update

Use the **clear mac address-table move update** privileged EXEC command to clear the mac address-table-move update-related counters.

## clear mac address-table move update

This command is supported only when the switch is running the metro IP access or metro access image.

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default is defined.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Examples** 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 was cleared by entering the **show mac address-table move update** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">mac address-table move update</a>	Configures MAC address-table move update on the switch.
	<a href="#">show mac address-table move update</a>	Displays the MAC address-table move update information on the switch.

# clear pagp

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

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



## Note

PAgP is available only on network node interfaces (NNIs) enhanced network interfaces (ENIs).

## Syntax Description

<i>channel-group-number</i>	(Optional) Channel group number. The range is 1 to 48.
<b>counters</b>	Clear traffic counters.

## Defaults

No default is defined.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

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

## Examples

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

```
Switch# clear pagp counters
```

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

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

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

## Related Commands

Command	Description
<a href="#">show pagp</a>	Displays PAgP channel-group information.

## clear policer cpu uni-eni counters

Use the **clear policer cpu uni-eni counters** privileged EXEC command to clear control-plane policer statistics. The control-plane policer drops or rate-limits control packets from user network interfaces (UNIs) and enhanced network interfaces (ENIs) to protect the CPU from overload.

```
clear policer cpu uni-eni counters {classification | drop}
```

### Syntax Description

<b>classification</b>	Clear control-plane policer classification counters that maintain statistics by feature.
<b>drop</b>	Clear all frame drop statistics maintained by the control-plane policer.

### Command Default

No default is defined.

### Command Modes

User EXEC

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

You can use this command to clear statistics maintained per feature or statistics about dropped frames. You can enter the **show platform policer cpu classification** or **show policer cpu uni drop** command to view feature statistics or dropped frames before and after you use the **clear** command.

### Related Commands

Command	Description
<a href="#">show platform policer cpu classification</a>	Displays CPU policer statistics per feature.
<a href="#">show policer cpu uni-eni</a>	Displays CPU policer information for the switch.



# clear port-security

Use the **clear port-security** privileged EXEC command to delete from the MAC address table all secure addresses or all secure addresses of a specific type (configured, dynamic, or sticky) on the switch or on an interface.

```
clear port-security {all | configured | dynamic | sticky} [[address mac-addr | interface
interface-id] [vlan {vlan-id | {access | voice} }]]
```

Syntax Description	
<b>all</b>	Delete all secure MAC addresses.
<b>configured</b>	Delete configured secure MAC addresses.
<b>dynamic</b>	Delete secure MAC addresses auto-learned by hardware.
<b>sticky</b>	Delete secure MAC addresses, either auto-learned or configured.
<b>address <i>mac-addr</i></b>	(Optional) Delete the specified dynamic secure MAC address.
<b>interface <i>interface-id</i></b>	(Optional) Delete all the dynamic secure MAC addresses on the specified physical port or VLAN.
<b>vlan</b>	(Optional) Delete the specified secure MAC address from the specified VLAN. Enter one of these options after you enter the <b>vlan</b> keyword: <ul style="list-style-type: none"> <li><b><i>vlan-id</i></b>—On a trunk port, specify the VLAN ID of the VLAN on which this address should be cleared.</li> <li><b>access</b>—On an access port, clear the specified secure MAC address on the access VLAN.</li> </ul>

**Defaults** No default is defined.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Examples** This example shows how to clear all secure addresses from the MAC address table:

```
Switch# clear port-security all
```

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

```
Switch# clear port-security configured address 0008.0070.0007
```

This example shows how to remove all the dynamic secure addresses learned on a specific interface:

```
Switch# clear port-security dynamic interface gigabitethernet0/1
```

This example shows how to remove all the dynamic secure addresses from the address table:

```
Switch# clear port-security dynamic
```

## ■ clear port-security

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

Related Commands	Command	Description
	<a href="#">switchport port-security</a>	Enables port security on an interface.
	<a href="#">switchport port-security mac-address <i>mac-address</i></a>	Configures secure MAC addresses.
	<a href="#">switchport port-security maximum <i>value</i></a>	Configures a maximum number of secure MAC addresses on a secure interface.
	<a href="#">show port-security</a>	Displays the port security settings defined for an interface or for the switch.

# clear rep counters

Use the **clear rep counters** privileged EXEC command to clear Resilient Ethernet Protocol (REP) counters for the specified interface or all interfaces.

**clear rep counters** [**interface** *interface-id*]

<b>Syntax Description</b>	<b>interface</b> <i>interface-id</i> (Optional) Specify a REP interface whose counters should be cleared.
---------------------------	---

<b>Defaults</b>	No default is defined.
-----------------	------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(50)SE	This command was introduced.

<b>Usage Guidelines</b>	<p>You can clear all REP counters by using the <b>clear rep counters</b> command, or you can clear only the counters for the interface by using the <b>clear rep counters interface</b> <i>interface-id</i> command.</p> <p>When you enter the <b>clear rep counters</b> command, only the counters visible in the output of the <b>show interface rep detail</b> command are cleared. SNMP visible counters are not cleared as they are read-only.</p>
-------------------------	---

<b>Examples</b>	This example shows how to clear all REP counters for all REP interfaces:
-----------------	--

```
Switch# clear rep counters
```

You can verify that REP information was deleted by entering the **show interfaces rep detail** privileged EXEC command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show interfaces rep detail</a>	Displays detailed REP configuration and status information.

# clear spanning-tree counters

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

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

<b>Syntax Description</b>	<p><b>interface</b> <i>interface-id</i> (Optional) Clear all spanning-tree counters on the specified interface. Valid interfaces include physical network node interfaces (NNIs), enhanced network interfaces (ENIs) on which spanning tree has been enabled, VLANs, and spanning-tree port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 48.</p> <p><b>Note</b> Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). Though visible in the command-line help, the command has no effect on UNIs or on ENIs on which STP is not enabled.</p>
---------------------------	--

<b>Defaults</b>	No default is defined.
-----------------	------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(44)EY</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(44)EY	This command was introduced.
Release	Modification				
12.2(44)EY	This command was introduced.				

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

<b>Examples</b>	This example shows how to clear spanning-tree counters for all STP ports:
-----------------	---

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

<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><a href="#">show spanning-tree</a></td> <td>Displays spanning-tree state information.</td> </tr> </tbody> </table>	Command	Description	<a href="#">show spanning-tree</a>	Displays spanning-tree state information.
Command	Description				
<a href="#">show spanning-tree</a>	Displays spanning-tree state information.				

# clear spanning-tree detected-protocols

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

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

## Syntax Description

**interface** *interface-id* (Optional) Restart the protocol migration process on the specified interface. Valid interfaces include physical network node interfaces (NNIs), enhanced network interfaces (ENIs) on which spanning tree is enabled, VLANs, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 48.

**Note** Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). Though visible in the command-line help, the command has no effect on UNIs or on ENIs on which STP is not enabled.

## Defaults

No default is defined.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

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

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

## Examples

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

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

■ clear spanning-tree detected-protocols

Related Commands	Command	Description
	<a href="#">show spanning-tree</a>	Displays spanning-tree state information.
	<a href="#">spanning-tree link-type</a>	Overrides the default link-type setting and enables rapid spanning-tree transitions to the forwarding state.

# clear vmmps statistics

Use the **clear vmmps statistics** privileged EXEC command to clear the statistics maintained by the VLAN Query Protocol (VQP) client.

## clear vmmps statistics

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default is defined.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Examples** This example shows how to clear VLAN Membership Policy Server (VMPS) statistics:

```
Switch# clear vmmps statistics
```

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

Related Commands	Command	Description
	<a href="#">show vmmps</a>	Displays the VQP version, reconfirmation interval, retry count, VMPS IP addresses, and the current and primary servers.

## conform-action

Use the **conform-action** policy-map class police configuration command to set multiple actions for a policy-map class for packets that conform to the committed information rate (CIR) or peak information rate (PIR) by having a rate less than the conform burst. Use the **no** form of this command to cancel the action or to return to the default action.

```
conform-action { drop | set-cos-transmit { new-cos-value | [cos | dscp | precedence] [table table-map name]} | set-dscp-transmit { new-dscp-value | [cos | dscp | precedence] [table table-map name]} | set-prec-transmit { new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-qos-transmit qos-group-value | transmit }
```

```
no conform-action { drop | set-cos-transmit { new-cos-value | [cos | dscp | precedence] [table table-map name]} | set-dscp-transmit { new-dscp-value | [cos | dscp | precedence] [table table-map name]} | set-prec-transmit { new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-qos-transmit qos-group-value | transmit }
```

### Syntax Description

<b>drop</b>	Drop the packet.
<b>set-cos-transmit</b> <i>new-cos-value</i>	Set a new class of service (CoS) value for the packet and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new CoS value is 0 to 7.
<b>set-dscp-transmit</b> <i>new-dscp-value</i>	Set a new Differentiated Services Code Point (DSCP) value for the packet and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new DSCP value is 0 to 63.
<b>set-prec-transmit</b> <i>new-precedence-value</i>	Set a new IP precedence value for the packet and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new IP precedence value is 0 to 7.
<b>set-qos-transmit</b> <i>qos-group-value</i>	Set a new quality of service (QoS) group value for the packet and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new QoS value is 0 to 99.
<b>cos</b>	(Optional) Set the packet marking specified in the preceding keyword based on the CoS value of the incoming packet, and send the packet. This specifies the <i>from-type</i> of the enhanced packet-marking action.
<b>dscp</b>	(Optional) Set the packet marking specified in the preceding keyword based on the DSCP value of the incoming packet, and send the packet. This specifies the <i>from-type</i> of the enhanced packet-marking action.
<b>precedence</b>	(Optional) Set the packet marking specified in the preceding keyword based on the IP precedence value of the incoming packet, and send the packet. This specifies the <i>from-type</i> of the enhanced packet-marking action.
<b>table</b> <i>table-map name</i>	(Optional) Used in conjunction with the preceding <i>from-type</i> keyword. Specify the table map to be used for the enhanced packet marking. The <i>to-type</i> of the action is marked based on the <i>from-type</i> parameter of the action using this table map.
<b>transmit</b>	(Optional) Send the packet unmodified.

### Defaults

The default conform action is to send the packet.



**Command Modes** Policy-map class police configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** You configure conform actions for packets when the packet rate is less than the configured conform burst.

If the conform action is set to **drop**, the exceed and violate actions are automatically set to **drop**.

You can configure conform-action marking by using enhanced packet marking to modify a QoS marking based on any incoming QoS marking and table maps. The switch also supports simultaneously marking multiple QoS parameters for the same class and configuring conform-action, exceed-action, and violate-action marking.

Access policy-map class police configuration mode by entering the **police** policy-map class command. See the **police** policy-map class configuration command for more information.

Use this command to set one or more conform actions for a traffic class.

**Examples** This example shows how configure multiple conform actions in a policy map that sets a committed information rate of 23000 bits per second (bps) and a conform burst rate of 10000 bps. The policy map includes multiple conform actions (for DSCP and for Layer 2 CoS) and an exceed action.

```
Switch(config)# policy-map map1
Switch(config-pmap)# class cos-set-1
Switch(config-pmap-c)# police cir 23000 bc 10000
Switch(config-pmap-c-police)# conform-action set-dscp-transmit 48
Switch(config-pmap-c-police)# conform-action set-cos-transmit 5
Switch(config-pmap-c-police)# exceed-action drop
Switch(config-pmap-c-police)# exit
```

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

Related Commands	Command	Description
	<b>class</b>	Defines a traffic classification match criteria for the specified class-map name.
	<b>exceed-action</b>	Defines the action to take on traffic that exceeds the CIR.
	<b>policy-map</b>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
	<b>police</b>	Defines a policer for classified traffic.
	<b>show policy-map</b>	Displays QoS policy maps.
	<b>violate-action</b>	Defines the action to take on traffic with a rate greater than the conform rate plus the exceed burst.

## copy logging onboard module

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

**copy logging onboard module** [*slot-number*] *destination*

Syntax Description	
<i>slot-number</i>	(Optional) The slot number is always 1 and is not relevant for the ME-3400E.
<i>destination</i>	<p>Specify the location on the local network or file system to which the system messages are copied.</p> <p>For <i>destination</i>, specify the destination on the local or network file system and the filename. These options are supported:</p> <ul style="list-style-type: none"> <li>The syntax for the local flash file system: <b>flash:/filename</b></li> <li>The syntax for the FTP: <b>ftp://username:password@host/filename</b></li> <li>The syntax for an HTTP server: <b>http://[[username:password]@]{hostname   host-ip}[/directory]/filename</b></li> <li>The syntax for the null file system: <b>null:/filename</b></li> <li>The syntax for the NVRAM: <b>nvrाम:/filename</b></li> <li>The syntax for the Remote Copy Protocol (RCP): <b>rcp://username@host/filename</b></li> <li>The syntax for the switch file system: <b>system:/filename</b></li> <li>The syntax for the TFTP: <b>tftp://[location]/directory/filename</b></li> <li>The syntax for the temporary file system: <b>tmpsys:/filename</b></li> </ul>

**Defaults** This command has no default setting.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

---

**Usage Guidelines**

For information about OBFL, see the [hw-module module logging onboard](#) global configuration command.

---

**Examples**

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

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

---

**Related Commands**

Command	Description
<a href="#">hw-module module logging onboard</a>	Enables OBFL.
<a href="#">show logging onboard</a>	Displays OBFL information.

## cpu traffic qos cos

Use the **cpu traffic qos cos** command in global configuration mode to configure quality of service (QoS) marking based on class of service (CoS) for control plane traffic. To return to the default value, use the **no** form of this command.

```
cpu traffic qos cos { cos_value | cos [table-map table-map-name] | dscp [table-map
table-map-name] | precedence [table-map table-map-name] }
```

```
no cpu traffic qos cos { cos_value | cos [table-map table-map-name] | dscp [table-map
table-map-name] | precedence [table-map table-map-name] }
```

### Syntax Description

<i>cos-value</i>	Specify a CoS value. The range is from 0 to 7. If no CoS value is configured, the protocol-specific default value for each packet is applied.
<b>cos</b>	Configure the CoS value based on the CoS value in the packet, using a table-map.
<b>table-map</b> <i>table-map-name</i>	Specify the table-map to use for marking the CPU traffic CoS based on the CoS value in the packet.
<b>dscp</b>	Configure the CoS value based on the DSCP value in the packet using a table-map.
<b>table-map</b> <i>table-map-name</i>	Specify the table-map to use for marking the CPU traffic CoS based on the DSCP value in the packet.
<b>precedence</b>	Configure the precedence value. The range is from 0 to 7.
<b>table-map</b> <i>table-map-name</i>	Specify the table-map to use for marking the CPU traffic CoS based on the IP-precedence value in the packet.

### Command Default

Control plane (CPU) traffic is not marked for QoS.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(52)SE	This command was introduced.

### Usage Guidelines

Configure any desired table-maps before configuring marking or queuing of CPU traffic.

This feature must be configured globally for a switch; it cannot be configured per-port or per-protocol.

Enter each **cpu traffic qos** marking action on a separate line.

The **cpu traffic qos cos** global configuration command configures CoS marking for CPU-generated traffic by using either a specific CoS value or a table map, but not both. A new configuration overwrites the existing configuration.

When the **cpu traffic qos cos** global configuration command is configured with table maps, you can configure two **map from** values at a time—CoS and either DSCP or precedence.

If the **cpu traffic qos cos** global configuration command is configured with only a **map from** value of IP-DSCP or IP-precedence:

- The CoS value of IP packets is mapped by using the IP-DSCP (or IP-precedence) value in the packet and the configured table map. Packets can be classified and queued by an output policy map based on the marked CoS value.
- The CoS value of non-IP packets remains unchanged.

If the **cpu traffic qos cos** global configuration command is configured with a **map from** value of CoS:

- The CoS value of IP packets is mapped by using the CoS value in the packet and the configured table map. Packets can be classified and queued by an output policy map based on the marked CoS value.
- The CoS value of non-IP packets is mapped by using the CoS value in the packet and the configured table map. Packets can be classified and queued by an output policy map based on the marked CoS value.

If the **cpu traffic qos cos** global configuration command is configured with a **map from** value of DSCP or precedence and CoS:

- The CoS value of IP packets is mapped by using the DSCP or precedence value in the packet and the configured table map. Packets can be classified and queued by an output policy map based on the marked CoS value.
- The CoS value of non-IP packets is mapped by using the CoS value in the packet and the configured table map. Packets can be classified and queued by an output policy map based on the marked CoS value.

## Examples

This example shows how to mark the CoS of CPU-generated IP traffic (including IP-SLA and TWAMP) based on the DSCP value in the packet and to configure egress queuing based on the CoS value.

The sample configuration has these results:

- All CPU-generated IP traffic is queued on the egress port based on the DSCP value and the configured output policy map called *output-policy*.
- All IP SLA or TWAMP probes with the DSCP value *ef* to simulate voice traffic are assigned to the *voice* class.
- All IP SLA or TWAMP probes with the DSCP values *af41*, *af42* and *af43* to simulate video traffic are assigned to the *video* class.
- All IP control protocol traffic with the DSCP values 48 and 56 are assigned to the *network-internetwork-control* class.
- The rest of the IP traffic is assigned to the default class.
- All CPU-generated non-IP traffic with CoS 5 is assigned to the *voice* class.
- All CPU-generated non-IP traffic with CoS 3 is assigned to the *video* class.
- All CPU-generated non-IP traffic with CoS 6 and 7 is assigned to the *network-internetwork-control* class.
- All CFM traffic with CoS 5 is assigned to the *voice* class.
- All CFM traffic with CoS 3 is assigned to the *video* class.
- All CFM traffic with CoS 6 and 7 is assigned to the *network-internetwork-control* class.

**Table Map:**

```
Switch(config)# table-map dscp-to-cos
Switch(config-tablemap)# map from 46 to 5
Switch(config-tablemap)# map from 48 to 6
Switch(config-tablemap)# map from 56 to 7
Switch(config-tablemap)# map from af41 to 3
Switch(config-tablemap)# map from af42 to 3
Switch(config-tablemap)# map from af43 to 3
Switch(config-tablemap)# default 0
Switch(config-tablemap)# end
```

**CPU QoS:**

```
Switch(config)# cpu traffic qos cos dscp table-map dscp-to-cos
Switch(config)# cpu traffic qos cos cos
```

**Class:**

```
Switch(config)# class-map match-any video
Switch(config-cmap)# match cos 3
Switch(config-cmap)# exit
```

```
Switch(config)# class-map match-any voice
Switch(config-cmap)# match cos 5
Switch(config-cmap)# exit
```

```
Switch(config)# class-map match-any network-internet-control
Switch(config-cmap)# match cos 6 7
Switch(config-cmap)# exit
```

**Policy:**

```
Switch(config)# policy-map output-policy
Switch(config-pmap)# class voice
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police cir 10000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video
Switch(config-pmap-c)# bandwidth percent 40
Switch(config-pmap-c)# exit
Switch(config-pmap)# class network-internet-control
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth percent 30
Switch(config-pmap-c)# exit
```

**Interface**

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output output-policy
Switch(config-pmap-c)# exit
```

**Related Commands**

Command	Description
<a href="#">class-map</a>	Configures a class map to be used for matching packets to a specified criteria and enters class-map configuration mode.
<a href="#">cpu traffic qos dscp</a>	Configures quality of service (QoS) marking based on DSCP for control plane traffic.
<a href="#">cpu traffic qos precedence</a>	Configure quality of service (QoS) marking based on precedence for control plane traffic.

Command	Description
<b>cpu traffic qos qos-group</b>	Maps <i>all</i> CPU-generated traffic to a single class in the output policy-maps without changing the class of service (CoS), IP differentiated services code point (DSCP), or IP-precedence packet markings.
<b>policy-map</b>	Configures a policy map that can be attached to multiple physical ports and enters policy-map configuration mode.
<b>show cpu traffic qos</b>	Displays the QoS markings configured for CPU traffic.
<b>show policy-map</b>	Displays QoS policy map information for the specified policy map name, interface, input or output policy maps, or policy-map class.
<b>show running-config</b>	Displays the configured class maps, policy maps, table maps, and aggregate policers.
<b>Related Commands</b>	Displays information for all configured table maps or the specified table map.
<b>table-map</b>	Configures quality of service (QoS) mapping and enters table-map configuration mode.

## cpu traffic qos dscp

Use the **cpu traffic qos dscp** command in global configuration mode to configure quality of service (QoS) marking based on a differentiated services code point (DSCP) value for control plane traffic. To return to the default value, use the **no** form of this command.

```
cpu traffic qos dscp {dscp_value | cos [table-map table-map-name]} | dscp [table-map
table-map-name] | precedence [table-map table-map-name]}
```

```
no cpu traffic qos dscp {dscp_value | cos [table-map table-map-name]} | dscp [table-map
table-map-name] | precedence [table-map table-map-name]}
```

### Syntax Description

<i>dscp-value</i>	Specify the IP-DSCP value. The range is from 0 to 63. If no IP-DSCP value is configured, the protocol-specific default value for each packet is applied.
<b>cos</b>	Configure the IP-DSCP value based on the CoS value in the packet, using a table map.
<b>table-map</b> <i>table-map-name</i>	Specify the table-map to use for marking the CPU traffic IP-DSCP based on the CoS value in the packet.
<b>dscp</b>	Configure the IP-DSCP value based on the IP-DSCP in the packet using a table map.
<b>table-map</b> <i>table-map-name</i>	Specify the table-map to use for marking the CPU traffic IP-DSCP based on the IP-DSCP value in the packet.
<b>precedence</b>	Configure the IP-precedence value based on the IP-precedence value in the packet using a table map.
<b>table-map</b> <i>table-map-name</i>	Specify the table-map to use for marking the CPU traffic IP-DSCP value based on the IP-precedence value in the packet.

### Command Default

Control plane (CPU) traffic is not marked for QoS.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(52)SE	This command was introduced.

### Usage Guidelines

This feature must be configured globally for a switch; it cannot be configured per-port or per-protocol. Enter each **cpu traffic qos** marking action on a separate line.

The **cpu traffic qos dscp** global configuration command configures IP-DSCP marking for CPU-generated IP traffic by using either a specific DSCP value or a table map, but not both. A new configuration overwrites the existing configuration.

The **cpu traffic qos dscp** and **cpu traffic qos precedence** global configuration commands are mutually exclusive. A new configuration overwrites the existing configuration.



When the **cpu traffic qos dscp** global configuration command is configured with table maps, you can configure only one **map from** value at a time—DSCP, precedence, or CoS. A new configuration overwrites the existing configuration. Packets marked by this command can be classified and queued by an output policy map based on the marked DSCP or precedence value.

You cannot configure a **map from** value of both DSCP and precedence. A new configuration overwrites the existing configuration.

## Examples

This example shows how to configure egress queuing based on the DSCP value of CPU-generated IP packets.

The sample configuration has these results:

- All CPU-generated IP traffic queues on the egress port, based on its IP DSCP value, and the configured output policy map *output-policy*.
- All IP SLA or TWAMP probes with the DSCP value *ef* to simulate voice traffic are assigned to the *voice* class.
- All IP SLA or TWAMP probes with the DSCP values *af41*, *af42* and *af43* to simulate video traffic are assigned to the *video* class.
- All IP control protocol traffic with the DSCP values *48* and *56* are assigned to the *network-internetnetwork-control* class.
- The rest of the IP traffic is assigned to the default class.
- All CPU-generated non-IP traffic is statically mapped to a fixed queue on the egress port.
- All CFM traffic is queued to the default class because there is no class based on CoS.

```
Switch(config)# cpu traffic qos dscp dscp
```

### Class:

```
Switch(config)# class-map match-any video  
Switch(config-cmap)# match ip dscp af41 af42 af43  
Switch(config-cmap)# exit
```

```
Switch(config)# class-map match-any voice  
Switch(config-cmap)# match ip dscp ef  
Switch(config-cmap)# exit
```

```
Switch(config)# class-map match-any network-internetnetwork-control  
Switch(config-cmap)# match ip dscp 48 56  
Switch(config-cmap)# exit
```

### Policy:

```
Switch(config)# policy-map output-policy  
Switch(config-pmap)# class voice  
Switch(config-pmap-c)# priority  
Switch(config-pmap-c)# police cir 10000000  
Switch(config-pmap-c)# exit  
Switch(config-pmap)# class video  
Switch(config-pmap-c)# bandwidth percent 40  
Switch(config-pmap-c)# exit  
Switch(config-pmap)# class network-internetnetwork-control  
Switch(config-pmap-c)# bandwidth percent 10  
Switch(config-pmap-c)# exit  
Switch(config-pmap)# class class-default  
Switch(config-pmap-c)# bandwidth percent 30  
Switch(config-pmap-c)# exit
```

**Interface**

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output output-policy
Switch(config-pmap-c)# exit
```

This example shows how to:

- Mark the DSCP value of CPU-generated IP traffic (including IP-SLA and TWAMP) based on the DSCP value in the packet.
- Mark the CoS of CPU-generated IP traffic (including IP-SLA and TWAMP) based on the DSCP value in the packet.
- Mark the CoS of CPU-generated non-IP traffic based on the CoS value in the packet.
- Mark all CPU-generated traffic with the QoS group.
- Configure egress queuing based on the QoS group.

The example has these results:

- All CPU-generated IP traffic with the DSCP values 46, 48, and 56 retain the existing markings.
- For all other CPU-generated IP packets, the DSCP value is reset to 0.
- All CPU-generated IP traffic with the DSCP values 46, 48, and 56 are mapped to corresponding CoS values of 5, 6, and 7, respectively.
- For all other CPU-generated IP packets, the CoS value resets to 0.
- All CPU-generated non-IP traffic with the CoS values of 5, 6, and 7 retain the existing markings.
- For all other CPU-generated non-IP packets, the CoS value resets to 0.
- All CPU-generated traffic goes through a single class called *cpu-traffic*. The *user-voice* classes *user-voice* and *user-video* are reserved for user traffic. As a result, CPU traffic and user traffic are separated into different queues on the egress port.

**Table-map**

```
Switch(config)# table-map dscp-to-cos
Switch(config-tablemap)# map from 46 to 5
Switch(config-tablemap)# map from 48 to 6
Switch(config-tablemap)# map from 56 to 7
Switch(config-tablemap)# default 0
Switch(config-tablemap)# end
```

```
Switch(config)# table-map dscp-to-dscp
Switch(config-tablemap)# map from 46 to 46
Switch(config-tablemap)# map from 48 to 48
Switch(config-tablemap)# map from 56 to 56
Switch(config-tablemap)# default 0
Switch(config-tablemap)# end
```

```
Switch(config)# table-map cos-to-cos
Switch(config-tablemap)# map from 5 to 5
Switch(config-tablemap)# map from 6 to 6
Switch(config-tablemap)# map from 7 to 7
Switch(config-tablemap)# default 0
Switch(config-tablemap)# end
```

**CPU QoS:**

```
Switch(config)# cpu traffic qos dscp dscp table-map dscp-to-dscp
Switch(config)# cpu traffic qos cos dscp table dscp-to-cos
Switch(config)# cpu traffic qos cos cos table cos-to-cos
Switch(config)# cpu traffic qos qos-group 50
```

**Class:**

```
Switch(config)# class-map match-any cpu-traffic
Switch(config-cmap)# match qos-group 50
Switch(config-cmap)# exit
```

```
Switch(config)# class-map match-any user-video
Switch(config-cmap)# match cos 3
Switch(config-cmap)# exit
```

```
Switch(config)# class-map match-any user-voice
Switch(config-cmap)# match cos 5
Switch(config-cmap)# exit
```

**Policy:**

```
Switch(config)# policy-map output-policy
Switch(config-pmap)# class user-voice
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police cir 10000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class user-video
Switch(config-pmap-c)# bandwidth percent 40
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cpu-traffic
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth percent 30
Switch(config-pmap-c)# exit
```

**Interface:**

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output output-policy
Switch(config-pmap-c)# exit
```

**Related Commands**

Command	Description
<b>class-map</b>	Configures a class map to be used for matching packets to a specified criteria and enters class-map configuration mode.
<b>cpu traffic qos cos</b>	Configures class of service (CoS) marking for control plane traffic.
<b>cpu traffic qos precedence</b>	Configure quality of service (QoS) marking based on precedence for control plane traffic.
<b>cpu traffic qos qos-group</b>	Maps <i>all</i> CPU-generated traffic to a single class in the output policy-maps without changing the class of service (CoS), IP differentiated services code point (DSCP), or IP-precedence packet markings.
<b>policy-map</b>	Configures a policy map that can be attached to multiple physical ports and enters policy-map configuration mode.
<b>show cpu traffic qos</b>	Displays the QoS markings configured for CPU traffic.
<b>show policy-map</b>	Displays QoS policy map information for the specified policy map name, interface, input or output policy maps, or policy-map class.

Command	Description
<b>show running-config</b>	Displays the configured class maps, policy maps, table maps, and aggregate policers.
<b>Related Commands</b>	Displays information for all configured table maps or the specified table map.
<b>table-map</b>	Configures quality of service (QoS) mapping and enters table-map configuration mode.

## cpu traffic qos precedence

Use the **cpu traffic qos precedence** command in global configuration mode to configure quality of service (QoS) marking for control plane traffic. To return to the default value, use the **no** form of this command.

```
cpu traffic qos precedence {precedence_value | cos [table-map table-map-name] | dscp
[table-map table-map-name] | precedence [table-map table-map-name]}
```

```
no cpu traffic qos precedence {precedence_value | cos [table-map table-map-name] | dscp
[table-map table-map-name] | precedence [table-map table-map-name]}
```

### Syntax Description

<i>precedence-value</i>	Configure the precedence value. The range is from 0 to 7. If no IP-precedence value is configured, the protocol-specific default value for each packet is applied.  <b>Note</b> You can substitute the following keywords for the numbers 0 to 7: <ul style="list-style-type: none"> <li>• routine (0)</li> <li>• priority (1)</li> <li>• immediate (2)</li> <li>• flash (3)</li> <li>• flash-override (4)</li> <li>• critical (5)</li> <li>• internet (6)</li> <li>• network (7)</li> </ul>
<b>cos</b>	Configure the CoS value based on the CoS value in the packet, using a table-map.
<b>table-map</b> <i>table-map-name</i>	Specify the table-map to use for marking the CPU traffic CoS based on the CoS value in the packet.
<b>dscp</b>	Configure the differentiated services code point (DSCP) value based on the IP-DSCP value in the packet, using a table-map.
<b>table-map</b> <i>table-map-name</i>	Specify the table-map to use for marking the CPU traffic precedence based on the DSCP value in the packet.
<b>precedence</b>	Configure the IP-precedence value based on the IP-precedence value in the packet, using a table-map.
<b>table-map</b> <i>table-map-name</i>	Specify the table-map to use for marking the CPU traffic precedence based on the precedence value in the packet.

### Command Default

Control plane (CPU) traffic is not marked for QoS.

### Command Modes

Global configuration

**Command History**

Release	Modification
12.2(52)SE	This command was introduced.

**Usage Guidelines**

This feature must be configured globally for a switch; it cannot be configured per-port or per-protocol. Enter each **cpu traffic qos** marking action on a separate line.

The **cpu traffic qos dscp** and **cpu traffic qos precedence** global configuration commands are mutually exclusive. A new configuration overwrites the existing configuration.

When the **cpu traffic qos precedence** global configuration command is configured with table maps, you can configure only one **map from** value at a time—DSCP, precedence, or CoS. A new configuration overwrites the existing configuration. Packets marked by this command can be classified and queued by an output policy map based on the marked precedence or DSCP value.

You cannot configure a **map from** value of both DSCP and precedence. A new configuration overwrites the existing configuration.

**Examples**

The following example shows how to mark the precedence based on the DSCP value in the packet and configure egress queuing based on the precedence value.

The example has these results:

- Marks the CPU-generated IP traffic with the DSCP value *48* to the precedence value *7*.
- Marks the other CPU-generated IP traffic to the precedence value *0*.
- Allows all other CPU-generated non-IP traffic to be processed by the default class.
- Queues CPU-generated IP traffic with precedence value *7* using class precedence *7*.
- Allows all other CPU-generated IP traffic to be processed by the default class.

**Table-map:**

```
switch(config)# table-map dscp-to-prec
switch(config-tablemap)# map from 48 to 7
switch(config-tablemap)# default 0
switch(config-tablemap)# end
```

**CPU QoS:**

```
switch(config)# cpu traffic qos precedence dscp table-map dscp-to-prec
```

**Class-maps:**

```
switch(config)# class-map prec7
switch(config-cmap)# match ip precedence 7
switch(config-cmap)# end
```

**Policy-maps:**

```
switch(config)# policy-map output-policy
switch(config-pmap)# class prec7
switch(config-pmap-c)# priority
switch(config-pmap-c)# end
```

**Interface:**

```
switch(config)# interface g1/0/1
switch(config-if)# service-policy output output-policy
switch(config-if)# exit
```

**Related Commands**

Command	Description
<a href="#">class-map</a>	Configures a class map to be used for matching packets to a specified criteria and enters class-map configuration mode.
<a href="#">cpu traffic qos cos</a>	Configures class of service (CoS) marking for control plane traffic.
<a href="#">cpu traffic qos dscp</a>	Configures quality of service (QoS) marking based on DSCP for control plane traffic.
<a href="#">cpu traffic qos qos-group</a>	Maps <i>all</i> CPU-generated traffic to a single class in the output policy-maps without changing the class of service (CoS), IP differentiated services code point (DSCP), or IP-precedence packet markings.
<a href="#">policy-map</a>	Configures a policy map that can be attached to multiple physical ports and enters policy-map configuration mode.
<a href="#">show cpu traffic qos</a>	Displays the QoS markings configured for CPU traffic.
<a href="#">show policy-map</a>	Displays QoS policy map information for the specified policy map name, interface, input or output policy maps, or policy-map class.
<a href="#">show running-config</a>	Displays the configured class maps, policy maps, table maps, and aggregate policers.
<a href="#">Related Commands</a>	Displays information for all configured table maps or the specified table map.
<a href="#">table-map</a>	Configures quality of service (QoS) mapping and enters table-map configuration mode.

## cpu traffic qos qos-group

Use the **cpu traffic qos qos-group** command in global configuration mode to map *all* CPU-generated traffic to a single class in the output policy-maps without changing the class of service (CoS), IP differentiated services code point (DSCP), or IP-precedence packet markings. To return to the default settings, use the **no** form of this command.

**cpu traffic qos qos-group** *qos-group-value*

**no cpu traffic qos qos-group** *qos-group-value*

<b>Syntax Description</b>	<i>qos-group-value</i>	Specify the QoS group number. Valid values are from 0 to 99.
---------------------------	------------------------	--

<b>Command Default</b>	Control plane (CPU) traffic is not marked for QoS.	
------------------------	--	--

<b>Command Modes</b>	Global configuration	
----------------------	----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(52)SE	This command was introduced.

<b>Usage Guidelines</b>	<p>This feature must be configured globally for a switch; it cannot be configured per-port or per-protocol. Enter each <b>cpu traffic qos</b> marking action on a separate line.</p> <p>The <b>cpu traffic qos qos-group</b> global configuration command can be used to configure QoS group marking for CPU-generated traffic only for a specific QoS group. The table-map option is not available.</p>
-------------------------	--

<b>Examples</b>	The following example shows how to mark all the CPU-generated traffic with a QoS-group and configure egress queuing based on that QoS-group.
-----------------	--

### CPU QoS:

```
switch(config)# cpu traffic qos qos-group 40
```

### Class-maps:

```
switch(config)# class-map group40
switch(config-cmap)# match qos-group 40
switch(config-cmap)# end
```

### Policy-maps:

```
switch(config)# policy-map output-policy
switch(config-pmap)# class group40
switch(config-pmap-c)# bandwidth percent 50
switch(config-pmap-c)# end
```



**Interface:**

```
Switch(config)# interface g1/0/1
Switch(config-if)# service-policy output output-policy
Switch(config-if)# exit
```

**Related Commands**

Command	Description
<a href="#">class-map</a>	Configures a class map to be used for matching packets to a specified criteria and enters class-map configuration mode.
<a href="#">cpu traffic qos cos</a>	Configures class of service (CoS) marking for control plane traffic.
<a href="#">cpu traffic qos dscp</a>	Configures quality of service (QoS) marking based on DSCP for control plane traffic.
<a href="#">cpu traffic qos precedence</a>	Configure quality of service (QoS) marking based on precedence for control plane traffic.
<a href="#">policy-map</a>	Configures a policy map that can be attached to multiple physical ports and enters policy-map configuration mode.
<a href="#">show cpu traffic qos</a>	Displays the QoS markings configured for CPU traffic.
<a href="#">show policy-map</a>	Displays QoS policy map information for the specified policy map name, interface, input or output policy maps, or policy-map class.
<a href="#">show running-config</a>	Displays the configured class maps, policy maps, table maps, and aggregate policers.
<a href="#">Related Commands</a>	Displays information for all configured table maps or the specified table map.
<a href="#">table-map</a>	Configures quality of service (QoS) mapping and enters table-map configuration mode.

## define interface-range

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

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

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

Syntax Description	
<i>macro-name</i>	Name of the interface-range macro; up to 32 characters.
<i>interface-range</i>	Interface range; for valid values for interface ranges, see “Usage Guidelines.”

**Defaults** This command has no default setting.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines**

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

A macro can contain up to five ranges.

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

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

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

Valid values for *type* and *interface*:

- vlan** *vlan-id*, where *vlan-id* is from 1 to 4094  
VLAN interfaces must have been configured with the **interface vlan** command (the **show running-config** privileged EXEC command displays the configured VLAN interfaces). VLAN interfaces not displayed by the **show running-config** command cannot be used in *interface-ranges*.
- port-channel** *port-channel-number*, where *port-channel-number* is from 1 to 48
- fastethernet** *module*{*first port*} - {*last port*}
- gigabitethernet** *module*{*first port*} - {*last port*}

For physical interfaces:

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

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

**gigabitethernet0/1 - 2**

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

**fastethernet0/3, gigabitethernet0/1 - 2**

**fastethernet0/3 -4, gigabitethernet0/1 - 2**

### Examples

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

```
Switch(config)# define interface-range macro1 fastethernet0/1 - 2, gigabitethernet0/1 - 2
```

### Related Commands

Command	Description
<a href="#">interface range</a>	Executes a command on multiple ports at the same time.
<b>show running-config</b>	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: <a href="http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html">http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html</a> Select the <b>Cisco IOS Commands Master List, Release 12.2</b> to navigate to the command.

# delete

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

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

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

Command Modes	
	Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines**

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

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

The prompting behavior depends on the setting of the **file prompt** global configuration command. By default, the switch prompts for confirmation on destructive file operations. For more information about this command, see the *Cisco IOS Command Reference for Release 12.1*.

**Examples**

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

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

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

Related Commands	Command	Description
	<a href="#">archive download-sw</a>	Downloads a new image to the switch and overwrites or keeps the existing image.

## deny (ARP access-list configuration)

Use the **deny** Address Resolution Protocol (ARP) access-list configuration command to deny an ARP packet based on matches against the DHCP bindings. Use the **no** form of this command to remove the specified access control entry (ACE) from the access list.

```
deny {[request] ip {any | host sender-ip | sender-ip sender-ip-mask} mac {any | host sender-mac | sender-mac sender-mac-mask} | response ip {any | host sender-ip | sender-ip sender-ip-mask} [{any | host target-ip | target-ip target-ip-mask}] mac {any | host sender-mac | sender-mac sender-mac-mask} [{any | host target-mac | target-mac target-mac-mask}] [log]
```

```
no deny {[request] ip {any | host sender-ip | sender-ip sender-ip-mask} mac {any | host sender-mac | sender-mac sender-mac-mask} | response ip {any | host sender-ip | sender-ip sender-ip-mask} [{any | host target-ip | target-ip target-ip-mask}] mac {any | host sender-mac | sender-mac sender-mac-mask} [{any | host target-mac | target-mac target-mac-mask}] [log]
```

### Syntax Description

<b>request</b>	(Optional) Define a match for the ARP request. When <b>request</b> is not specified, matching is performed against all ARP packets.
<b>ip</b>	Specify the sender IP address.
<b>any</b>	Deny any IP or MAC address.
<b>host</b> <i>sender-ip</i>	Deny the specified sender IP address.
<i>sender-ip sender-ip-mask</i>	Deny the specified range of sender IP addresses.
<b>mac</b>	Deny the sender MAC address.
<b>host</b> <i>sender-mac</i>	Deny a specific sender MAC address.
<i>sender-mac sender-mac-mask</i>	Deny the specified range of sender MAC addresses.
<b>response ip</b>	Define the IP address values for the ARP responses.
<b>host</b> <i>target-ip</i>	Deny the specified target IP address.
<i>target-ip target-ip-mask</i>	Deny the specified range of target IP addresses.
<b>mac</b>	Deny the MAC address values for the ARP responses.
<b>host</b> <i>target-mac</i>	Deny the specified target MAC address.
<i>target-mac target-mac-mask</i>	Deny the specified range of target MAC addresses.
<b>log</b>	(Optional) Log a packet when it matches the ACE.

### Defaults

There are no default settings. However, at the end of the ARP access list, there is an implicit **deny ip any mac any** command.

### Command Modes

ARP access-list configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

## deny (ARP access-list configuration)

**Usage Guidelines**

You can add deny clauses to drop ARP packets based on matching criteria.

**Examples**

This example shows how to define an ARP access list and to deny both ARP requests and ARP responses from a host with an IP address of 1.1.1.1 and a MAC address of 0000.0000.abcd:

```
Switch(config)# arp access-list static-hosts
Switch(config-arp-nacl)# deny ip host 1.1.1.1 mac host 0000.0000.abcd
Switch(config-arp-nacl)# end
```

You can verify your settings by entering the **show arp access-list** privileged EXEC command.

**Related Commands**

Command	Description
<a href="#">arp access-list</a>	Defines an ARP access control list (ACL).
<a href="#">ip arp inspection filter vlan</a>	Permits ARP requests and responses from a host configured with a static IP address.
<a href="#">permit (ARP access-list configuration)</a>	Permits an ARP packet based on matches against the DHCP bindings.
<a href="#">show arp access-list</a>	Displays detailed information about ARP access lists.

## deny (IPv6 access-list configuration)

Use the **deny** command in IPv6 access list configuration mode to set deny conditions for an IPv6 access list. Use the **no** form of this command to remove the deny conditions.

```
deny {protocol} {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator
[port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address}
[operator [port-number]] [dscp value] [fragments] [log] [log-input] [routing] [sequence
value] [time-range name]
```

```
no deny {protocol} {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator
[port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address}
[operator [port-number]] [dscp value] [fragments] [log] [log-input] [routing] [sequence
value] [time-range name]
```

### Internet Control Message Protocol

```
deny icmp {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator
[port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address}
[operator [port-number]] [icmp-type [icmp-code] | icmp-message] [dscp value] [log]
[log-input] [routing] [sequence value] [time-range name]
```

### Transmission Control Protocol

```
deny tcp {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator
[port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address}
[operator [port-number]] [ack] [dscp value] [established] [fin] [log] [log-input] [neq {port |
protocol}] [psh] [range {port | protocol}] [rst] [routing] [sequence value] [syn] [time-range
name] [urg]
```

### User Datagram Protocol

```
deny udp {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator
[port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address}
[operator [port-number]] [dscp value] [log] [log-input] [neq {port | protocol}] [range {port |
protocol}] [routing] [sequence value] [time-range name]
```



#### Note

This command is available only if the switch is running the metro IP access image and you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

#### Syntax Description

<i>protocol</i>	Name or number of an Internet protocol. It can be one of the keywords <b>ahp</b> , <b>esp</b> , <b>icmp</b> , <b>ipv6</b> , <b>pcp</b> , <b>setp</b> , <b>tcp</b> , or <b>udp</b> , or an integer in the range from 0 to 255 representing an IPv6 protocol number.
<i>source-ipv6-prefix/prefix-length</i>	The source IPv6 network or class of networks about which to set deny conditions.  This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
<b>any</b>	An abbreviation for the IPv6 prefix <code>::/0</code> .

<b>host</b>	The source IPv6 host address for which to set deny conditions.
<i>source-ipv6-address</i>	This <i>source-ipv6-address</i> argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
<i>operator [port-number]</i>	<p>(Optional) Specify an operator that compares the source or destination ports of the specified protocol. Operators are <b>lt</b> (less than), <b>gt</b> (greater than), <b>eq</b> (equal), <b>neq</b> (not equal), and <b>range</b> (inclusive range).</p> <p>If the operator is positioned after the <i>source-ipv6-prefix/prefix-length</i> argument, it must match the source port.</p> <p>If the operator is positioned after the <i>destination-ipv6-prefix/prefix-length</i> argument, it must match the destination port.</p> <p>The <b>range</b> operator requires two port numbers. All other operators require one port number.</p> <p>The optional <i>port-number</i> argument is a decimal number or the name of a TCP or a UDP port. A port number is a number from 0 to 65535. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.</p>
<i>destination-ipv6-prefix/prefix-length</i>	<p>The destination IPv6 network or class of networks for which to set deny conditions.</p> <p>This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</p>
<b>host</b>	The destination IPv6 host address for which to set deny conditions.
<i>destination-ipv6-address</i>	This <i>destination-ipv6-address</i> argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
<b>dscp value</b>	(Optional) Match a differentiated services code point value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63.
<b>fragments</b>	(Optional) Match non-initial fragmented packets where the fragment extension header contains a non-zero fragment offset. The <b>fragments</b> keyword is an option only if the protocol is <b>ipv6</b> and the <i>operator [port-number]</i> arguments are not specified.
<b>log</b>	<p>(Optional) Send an informational logging message to the console about the packet that matches the entry. (The level of messages sent to the console is controlled by the <b>logging console</b> command.)</p> <p>The message includes the access list name and sequence number, whether the packet was denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets denied in the prior 5-minute interval.</p> <p><b>Note</b> Logging is not supported for port ACLs.</p>
<b>log-input</b>	(Optional) Provide the same function as the <b>log</b> keyword, but the logging message also includes the receiving interface.
<b>routing</b>	(Optional) Match packets with the routing extension header.



<b>sequence</b> <i>value</i>	(Optional) Specify the sequence number for the access list statement. The acceptable range is from 1 to 4294967295.
<b>time-range</b> <i>name</i>	(Optional) Specify the time range that applies to the deny statement. The name of the time range and its restrictions are specified by the <b>time-range</b> and <b>absolute</b> or <b>periodic</b> commands, respectively.
<i>icmp-type</i>	(Optional) Specify an ICMP message type for filtering ICMP packets. ICMP packets can be filtered by an ICMP message type. The type is a number from 0 to 255.
<i>icmp-code</i>	(Optional) Specify an ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
<i>icmp-message</i>	(Optional) Specify an ICMP message name for filtering ICMP packets. ICMP packets can be filtered by an ICMP message name or an ICMP message type and code. The possible names are listed in the “Usage Guidelines” section.
<b>ack</b>	(Optional) Only for the TCP protocol: Acknowledgment (ACK) bit set.
<b>established</b>	(Optional) Only for the TCP protocol: Means the connection has been established. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.
<b>fin</b>	(Optional) Only for the TCP protocol: Fin bit set; no more data from sender.
<b>neq</b> { <i>port</i>   <i>protocol</i> }	(Optional) Match only packets that are not on a given port number.
<b>psh</b>	(Optional) Only for the TCP protocol: Push function bit set.
<b>range</b> { <i>port</i>   <i>protocol</i> }	(Optional) Match only packets in the range of port numbers.
<b>rst</b>	(Optional) Only for the TCP protocol: Reset bit set.
<b>syn</b>	(Optional) Only for the TCP protocol: Synchronize bit set.
<b>urg</b>	(Optional) Only for the TCP protocol: Urgent pointer bit set.

**Note**

Although visible in the command-line help strings, the **flow-label**, **routing**, and **undetermined-transport** keywords are not supported.

**Defaults**

No IPv6 access list is defined.

**Command Modes**

IPv6 access list configuration

**Command History**

Release	Modification
12.2(50)SE	This command was introduced.

**Usage Guidelines**

The **deny** (IPv6 access-list configuration mode) command is similar to the **deny** (IPv4 access-list configuration mode) command, but it is IPv6-specific.

Use the **deny** (IPv6) command after the **ipv6 access-list** command to enter IPv6 access list configuration mode and to define the conditions under which a packet passes the access list.

Specifying IPv6 for the *protocol* argument matches the IPv6 header of the packet.

By default, the first statement in an access list is number 10, and the subsequent statements are numbered in increments of 10.

You can add **permit**, **deny**, or **remark** statements to an existing access list without re-entering the entire list. To add a new statement somewhere other than at the end of the list, create a new statement with an appropriate entry number between two existing entry numbers to show where it belongs.

**Note**

Every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. The two **permit** conditions allow ICMPv6 neighbor discovery. To disallow ICMPv6 neighbor discovery and to deny **icmp any any nd-na** or **icmp any any nd-ns**, there must be an explicit **deny** entry in the ACL. For the three implicit statements to take effect, an IPv6 ACL must contain at least one entry.

The IPv6 neighbor discovery process uses the IPv6 network layer service. Therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, uses a separate data-link layer protocol. Therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Both the *source-ipv6-prefix/prefix-length* and *destination-ipv6-prefix/prefix-length* arguments are used for traffic filtering. (The *source* prefix filters traffic based upon its source; the *destination* prefix filters traffic based upon its destination.)

The switch supports IPv6 address matching for a full range of prefix lengths.

The **fragments** keyword is an option only if the protocol is **ipv6** and the *operator [port-number]* arguments are not specified.

This is a list of ICMP message names:

beyond-scope	destination-unreachable
echo-reply	echo-request
header	hop-limit
mld-query	mld-reduction
mld-report	nd-na
nd-ns	next-header
no-admin	no-route
packet-too-big	parameter-option
parameter-problem	port-unreachable
reassembly-timeout	renum-command
renum-result	renum-seq-number
router-advertisement	router-renumbering
router-solicitation	time-exceeded
unreachable	

**Examples**

This example configures the IPv6 access list named CISCO and applies the access list to outbound traffic on a Layer 3 interface. The first deny entry prevents all packets that have a destination TCP port number greater than 5000 from leaving the interface. The second deny entry prevents all packets that have a source UDP port number less than 5000 from leaving the interface. The second deny also logs all matches to the console. The first permit entry permits all ICMP packets to leave the interface. The second permit entry permits all other traffic to leave the interface. The second permit entry is necessary because an implicit deny-all condition is at the end of each IPv6 access list.

```
Switch(config)# ipv6 access-list CISCO
Switch(config-ipv6-acl)# deny tcp any any gt 5000
Switch config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# permit any any
Switch(config-ipv6-acl)# exit
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter CISCO out
```

**Related Commands**

Command	Description
<a href="#">ipv6 access-list</a>	Defines an IPv6 access list and enters IPv6 access list configuration mode.
<a href="#">ipv6 traffic-filter</a>	Filters incoming or outgoing IPv6 traffic on an interface.
<a href="#">permit (IPv6 access-list configuration)</a>	Sets permit conditions for an IPv6 access list.
<a href="#">show ipv6 access-list</a>	Displays the contents of all current IPv6 access lists.

## deny (MAC access-list configuration)

Use the **deny** MAC access-list configuration command to prevent non-IP traffic from being forwarded if the conditions are matched. Use the **no** form of this command to remove a deny condition from the named MAC access list.

```
{deny | permit} {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr |
dst-MAC-addr mask} [type mask | aarp | amber | cos cos | 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]
```

```
no {deny | permit} {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr |
dst-MAC-addr mask} [type mask | aarp | amber | cos cos | 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]
```

### Syntax Description

<b>any</b>	Keyword to specify to deny any source or destination MAC address.
<b>host</b> <i>src MAC-addr</i>   <i>src-MAC-addr mask</i>	Define 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.
<b>host</b> <i>dst-MAC-addr</i>   <i>dst-MAC-addr mask</i>	Define 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) Use the Ethertype number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet.  The <i>type</i> is 0 to 65535, specified in hexadecimal.  The <i>mask</i> is a mask of <i>don't care</i> bits applied to the Ethertype before testing for a match.
<b>aarp</b>	(Optional) Select Ethertype AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
<b>amber</b>	(Optional) Select EtherType DEC-Amber.
<b>cos</b> <i>cos</i>	(Optional) Select 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 <b>cos</b> option is configured.
<b>dec-spanning</b>	(Optional) Select EtherType Digital Equipment Corporation (DEC) spanning tree.
<b>decnet-iv</b>	(Optional) Select EtherType DECnet Phase IV protocol.
<b>diagnostic</b>	(Optional) Select EtherType DEC-Diagnostic.
<b>dsm</b>	(Optional) Select EtherType DEC-DSM.
<b>etype-6000</b>	(Optional) Select EtherType 0x6000.
<b>etype-8042</b>	(Optional) Select EtherType 0x8042.
<b>lat</b>	(Optional) Select EtherType DEC-LAT.
<b>larc-sca</b>	(Optional) Select EtherType DEC-LARC-SCA.

<b>lsap</b> <i>lsap-number mask</i>	(Optional) Use the LSAP number (0 to 65535) of a packet with IEEE 802.2 encapsulation to identify the protocol of the packet. <i>mask</i> is a mask of <i>don't care</i> bits applied to the LSAP number before testing for a match.
<b>mop-console</b>	(Optional) Select EtherType DEC-MOP Remote Console.
<b>mop-dump</b>	(Optional) Select EtherType DEC-MOP Dump.
<b>msdos</b>	(Optional) Select EtherType DEC-MSDOS.
<b>mumps</b>	(Optional) Select EtherType DEC-MUMPS.
<b>netbios</b>	(Optional) Select EtherType DEC- Network Basic Input/Output System (NETBIOS).
<b>vines-echo</b>	(Optional) Select EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
<b>vines-ip</b>	(Optional) Select EtherType VINES IP.
<b>xns-idp</b>	(Optional) Select EtherType Xerox Network Systems (XNS) protocol suite (0 to 65535), an arbitrary Ethertype in decimal, hexadecimal, or octal.

**Note**

Though visible in the command-line help strings, **appletalk** is not supported as a matching condition.

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 [Table 2-1](#).

**Table 2-1 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

**Defaults**

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
12.2(44)EY	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.

**Note**

For more information about named MAC extended access lists, see the software configuration guide for this release.

**Examples**

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.

```
Switch(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:

```
Switch(config-ext-macl)# no deny any 00c0.00a0.03fa 0000.0000.0000 netbios.
```

This example denies all packets with Ethertype 0x4321:

```
Switch(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
<b>mac access-list extended</b>	Creates an access list based on MAC addresses for non-IP traffic.
<b>permit (MAC access-list configuration)</b>	Permits non-IP traffic to be forwarded if conditions are matched.
<b>show access-lists</b>	Displays access control lists configured on a switch.

# diagnostic monitor

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

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

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

**diagnostic monitor syslog**

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

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

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

**no diagnostic monitor syslog**

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

## Syntax Description

<b>interval test</b>	Configure the interval between tests.
<b>test</b>	Specify the tests to be run.
<i>name</i>	Specify the test name. To display the test names in the test-ID list, enter the <b>show diagnostic content</b> privileged EXEC command.
<i>test-id</i>	Specify the ID number of the test. The range is from 1 to 6. To display the test numbers in the test-ID list, enter the <b>show diagnostic content</b> privileged EXEC command.
<i>test-id-range</i>	Specify more than one test with the range of test ID numbers. Enter the range as integers separated by a comma and a hyphen (for example, 1,3-6 specifies test IDs 1, 3, 4, 5, and 6). To display the test numbers in the test-ID list, enter the <b>show diagnostic content</b> privileged EXEC command.
<b>all</b>	Specify all of the diagnostic tests.
<i>hh:mm:ss</i>	Configure the monitoring interval in hours, minutes, and seconds. <ul style="list-style-type: none"> <li><i>hh</i>—Enter the hours from 0 to 24.</li> <li><i>mm</i>—Enter the minutes from 0 to 60.</li> <li><i>ss</i>—Enter the seconds from 0 to 60.</li> </ul>
<i>milliseconds</i>	Configure the monitoring interval (test time) in milliseconds (ms). The range is from 0 to 999 ms.
<i>day</i>	Configure the monitoring interval in the number of days between tests. The range is from 0 to 20 days.
<b>syslog</b>	Enable the generation of a syslog message when a health-monitoring test fails.
<b>threshold test</b>	Configure the failure threshold.
<b>failure count</b> <i>count</i>	Set the failure threshold count. The range for <i>count</i> is from 0 to 99.

## Defaults

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

## ■ diagnostic monitor

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

### Usage Guidelines

- You must configure the failure threshold and the interval between tests before enabling diagnostic monitoring.
- Enter the **diagnostic monitor test 1** command to enable diagnostic monitoring.
- When you enter the **diagnostic monitor test** {*name* | *test-id* | *test-id-range* | **all**} command, you must isolate network traffic by disabling all connected ports.
- Do not send test packets during the test.

### Examples

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

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

### Related Commands

Command	Description
<a href="#">show diagnostic</a>	Displays online diagnostic test results.



# diagnostic schedule test

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

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

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

## Syntax Description

<i>name</i>	Specify the name of the test. To display the test names in the test-ID list, enter the <b>show diagnostic content</b> privileged EXEC command.
<i>test-id</i>	Specify the ID number of the test. The range is from 1 to 6. To display the test numbers in the test-ID list, enter the <b>show diagnostic content</b> privileged EXEC command.
<i>test-id-range</i>	Specify more than one test with the range of test ID numbers. Enter the range as integers separated by a comma and a hyphen (for example, 1,3-6 specifies test IDs 1, 3, 4, 5, and 6). To display the test numbers in the test-ID list, enter the <b>show diagnostic content</b> privileged EXEC command.
<b>all</b>	Specify all of the diagnostic tests.
<b>basic</b>	Specify the basic on-demand diagnostic tests.
<b>non-disruptive</b>	Specify the nondisruptive health-monitoring tests.
<b>daily</b> <i>hh:mm</i>	Specify the daily scheduling of the diagnostic tests. <i>hh:mm</i> —Enter the time as a 2-digit number (for a 24-hour clock) for hours:minutes; the colon (:) is required, such as 12:30.
<b>on</b> <i>mm dd yyyy hh:mm</i>	Specify the scheduling of the diagnostic tests on a specific day and time. For <i>mm dd yyyy</i> : <ul style="list-style-type: none"> <li><i>mm</i>—Spell out the month, such as January, February, and so on, with upper-case or lower-case characters.</li> <li><i>dd</i>—Enter the day as a 2-digit number, such as 03 or 16.</li> <li><i>yyyy</i>—Enter the year as a 4-digit number, such as 2008.</li> </ul>
<b>weekly</b> <i>day-of-week hh:mm</i>	Specify the weekly scheduling of the diagnostic tests. <i>day-of-week</i> —Spell out the day of the week, such as Monday, Tuesday, and so on, with upper-case or lower-case characters.

## Defaults

This command has no default settings.

## Command Modes

Global configuration

## ■ diagnostic schedule test

**Command History**

Release	Modification
12.2(44)EY	This command was introduced.

**Examples**

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

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

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

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

**Related Commands**

Command	Description
<a href="#">show diagnostic</a>	Displays online diagnostic test results.

# diagnostic start test

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

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

Syntax Description	
<i>name</i>	Specify the name of the test. To display the test names in the test-ID list, enter the <b>show diagnostic content</b> privileged EXEC command.
<i>test-id</i>	Specify the ID number of the test. The range is from 1 to 6. To display the test numbers in the test-ID list, enter the <b>show diagnostic content</b> privileged EXEC command.
<i>test-id-range</i>	Specify more than one test with the range of test ID numbers. Enter the range as integers separated by a comma and a hyphen (for example, 1,3-6 specifies test IDs 1, 3, 4, 5, and 6). To display the test numbers in the test-ID list, enter the <b>show diagnostic content</b> privileged EXEC command.
<b>all</b>	Specify all the diagnostic tests.
<b>basic</b>	Specify the basic on-demand diagnostic tests.
<b>non-disruptive</b>	Specify the nondisruptive health-monitoring tests.

**Defaults** This command has no default setting.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

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

The switch supports these tests:

```
ID   Test Name [On-Demand Test Attributes]
---   -
```

1	TestPortAsicStackPortLoopback	[B*N****]
2	TestPortAsicLoopback	[B*D*R**]
3	TestPortAsicCam	[B*D*R**]
4	TestPortAsicRingLoopback	[B*D*R**]
5	TestMicRingLoopback	[B*D*R**]
6	TestPortAsicMem	[B*D*R**]

```
---
```

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

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

### Examples

This example shows how to start diagnostic test 1:

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

This example shows how to start diagnostic test 2. Running this test disrupts the normal system operation and then reloads the switch.

```
Switch# diagnostic start test 2
Running test(s) 2 will cause the switch under test to reload after completion of
the test list.
Running test(s) 2 may disrupt normal system operation
Do you want to continue? [no]: y
Switch#
00:00:25: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan
00:00:29: %SYS-5-CONFIG_I: Configured from memory by console
00:00:30: %DIAG-6-TEST_RUNNING : Running TestPortAsicLoopback{ID=2} ...
00:00:30: %DIAG-6-TEST_OK: TestPortAsicLoopback{ID=2} has completed successfully
```

### Related Commands

Command	Description
<a href="#">show diagnostic</a>	Displays online diagnostic test results.

# dot1x default

Use the **dot1x default** interface configuration command to reset the configurable IEEE 802.1x parameters to their default values.

## dot1x default

### Syntax Description

This command has no arguments or keywords.

### Defaults

These are the default values:

- The per-port IEEE 802.1x protocol enable state is disabled (force-authorized).
- The number of seconds between re-authentication attempts is 3600 seconds.
- The periodic re-authentication is disabled.
- The quiet period is 60 seconds.
- The retransmission time is 30 seconds.
- The maximum retransmission number is 2 times.
- The host mode is single host.
- The client timeout period is 30 seconds.
- The authentication server timeout period is 30 seconds.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Examples

This example shows how to reset the configurable IEEE 802.1x parameters on a port:

```
Switch(config-if)# dot1x default
```

You can verify your settings by entering the **show dot1x [interface interface-id]** privileged EXEC command.

### Related Commands

Command	Description
<b>show dot1x [interface interface-id]</b>	Displays IEEE 802.1x status for the specified port.

## dot1x host-mode

Use the **dot1x host-mode** interface configuration command to allow a single host (client) or multiple hosts on an IEEE 802.1x-authorized port that has the **dot1x port-control** interface configuration command set to **auto**. Use the **no** form of this command to return to the default setting.

```
dot1x host-mode { multi-host | single-host }
```

```
no dot1x host-mode [multi-host | single-host]
```



### Note

Although visible in the command-line interface help, the **multi-domain** keyword is not supported.

### Syntax Description

<b>multi-host</b>	Enable multiple-hosts mode on the switch.
<b>single-host</b>	Enable single-host mode on the switch.

### Defaults

The default is single-host mode.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

Use this command to limit an IEEE 802.1x-enabled port to a single client or to attach multiple clients to an IEEE 802.1x-enabled port. In multiple-hosts mode, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (re-authentication fails or an Extensible Authentication Protocol over LAN [EAPOL]-logoff message is received), all attached clients are denied access to the network.

Before entering this command, make sure that the **dot1x port-control** interface configuration command is set to **auto** for the specified port.

The **dot1x host-mode multi-domain** interface configuration command is not supported on the switch. Configuring this command on an interface causes the interface to go into the error-disabled state.

### Examples

This example shows how to enable IEEE 802.1x globally, to enable IEEE 802.1x on a port, and to enable multiple-hosts mode:

```
Switch(config)# dot1x system-auth-control
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
```

You can verify your settings by entering the **show dot1x [interface interface-id]** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<code>show dot1x [interface <i>interface-id</i>]</code>	Displays IEEE 802.1x status for the specified port.

# dot1x initialize

Use the **dot1x initialize** privileged EXEC command to manually return the specified IEEE 802.1x-enabled port to an unauthorized state before initiating a new authentication session on the port.

**dot1x initialize interface** *interface-id*

## Syntax Description

**interface** *interface-id* Port to be initialized.

## Defaults

There is no default setting.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

Use this command to initialize the IEEE 802.1x state machines and to set up a fresh environment for authentication. After you enter this command, the port status becomes unauthorized.

There is no **no** form of this command.

## Examples

This example shows how to manually initialize a port:

```
Switch# dot1x initialize interface gigabitethernet0/2
```

You can verify the unauthorized port status by entering the **show dot1x [interface interface-id]** privileged EXEC command.

## Related Commands

Command	Description
<b>show dot1x [interface interface-id]</b>	Displays IEEE 802.1x status for the specified port.



# dot1x max-reauth-req

Use the **dot1x max-reauth-req** interface configuration command to set the maximum number of times that the switch restarts the authentication process before a port transitions to the unauthorized state. Use the **no** form of this command to return to the default setting.

**dot1x max-reauth-req** *count*

**no dot1x max-reauth-req**

## Syntax Description

<i>count</i>	Sets the number of times that switch retransmits EAPOL-Identity-Request frames to start the authentication process before the port changes to the unauthorized state. If a non-802.1x capable device is connected to a port, the switch retries two authentication attempts by default. If a guest VLAN is configured on the port, after two re-authentication attempts, the port is authorized on the guest vlan by default. The range is 1 to 10. The default is 2.
--------------	---

## Defaults

The default is 2 times.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	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.

## Examples

This example shows how to set 4 as the number of times that the switch restarts the authentication process before the port transitions to the unauthorized state:

```
Switch(config-if)# dot1x max-reauth-req 4
```

You can verify your settings by entering the **show dot1x [interface interface-id]** privileged EXEC command.

## Related Commands

Command	Description
<a href="#">dot1x max-req</a>	Sets the maximum number of times that the switch forwards an EAP frame (assuming that no response is received) to the authentication server before restarting the authentication process.

Command	Description
<b>dot1x timeout tx-period</b>	Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending the request.
<b>show dot1x</b> [interface <i>interface-id</i> ]	Displays IEEE 802.1x status for the specified port.

## dot1x max-req

Use the **dot1x max-req** interface configuration command to set the maximum number of times that the switch sends an Extensible Authentication Protocol (EAP) frame from the authentication server (assuming that no response is received) to the client before restarting the authentication process. Use the **no** form of this command to return to the default setting.

**dot1x max-req** *count*

**no dot1x max-req**

### Syntax Description

<i>count</i>	Number of times that the switch attempts to retransmit EAPOL DATA packets before restarting the authentication process. For example, if a problem occurs on a supplicant during the authentication process, the authenticator will re-transmit data requests two times before stopping the process. The range is 1 to 10; the default is 2
--------------	--

### Defaults

The default is 2 times.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(44)EY	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.

### Examples

This example shows how to set 5 as the number of times that the switch sends an EAP frame from the authentication server before restarting the authentication process:

```
Switch(config-if)# dot1x max-req 5
```

You can verify your settings by entering the **show dot1x [interface interface-id]** privileged EXEC command.

### Related Commands

Command	Description
<b>dot1x timeout tx-period</b>	Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending the request.
<b>show dot1x [interface interface-id]</b>	Displays IEEE 802.1x status for the specified port.

## dot1x port-control

Use the **dot1x port-control** interface configuration command to enable manual control of the authorization state of the port. Use the **no** form of this command to return to the default setting.

**dot1x port-control {auto | force-authorized | force-unauthorized}**

**no dot1x port-control**

Syntax Description	auto	force-authorized	force-unauthorized
	Enable IEEE 802.1x authentication on the port and cause the port to change to the authorized or unauthorized state based on the IEEE 802.1x authentication exchange between the switch and the client.	Disable IEEE 802.1x authentication on the port and cause the port to change to the authorized state without an authentication exchange. The port sends and receives normal traffic without IEEE 802.1x-based authentication of the client.	Deny all access through this port by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the port.

**Defaults** The default is force-authorized.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** You must globally enable IEEE 802.1x on the switch by using the **dot1x system-auth-control** global configuration command before enabling IEEE 802.1x on a specific port.

The IEEE 802.1x protocol is supported on Layer 2 static-access ports and Layer 3 routed ports.

You can use the **auto** keyword only if the port is not configured as one of these:

- Trunk port—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, an error message appears, and the port mode is not changed.
- Dynamic-access ports—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.
- EtherChannel port—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 on an EtherChannel port, an error message appears, and IEEE 802.1x is not enabled.

- Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) destination ports—You can enable IEEE 802.1x on a port that is a SPAN or RSPAN destination port. However, IEEE 802.1x is disabled until the port is removed as a SPAN or RSPAN destination. You can enable IEEE 802.1x on a SPAN or RSPAN source port.

To globally disable IEEE 802.1x on the switch, use the **no dot1x system-auth-control** global configuration command. To disable IEEE 802.1x on a specific port, use the **no dot1x port-control** interface configuration command.

---

**Examples**

This example shows how to enable IEEE 802.1x on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x port-control auto
```

You can verify your settings by entering the **show dot1x [interface interface-id]** privileged EXEC command.

---

**Related Commands**

Command	Description
<b>show dot1x [interface interface-id]</b>	Displays IEEE 802.1x status for the specified port.

## dot1x re-authenticate

Use the **dot1x re-authenticate** privileged EXEC command to manually initiate a re-authentication of the specified IEEE 802.1x-enabled port.

**dot1x re-authenticate interface** *interface-id*

<b>Syntax Description</b>	<b>interface</b> <i>interface-id</i> Module and port number of the interface to re-authenticate.
---------------------------	--

<b>Defaults</b>	There is no default setting.
-----------------	------------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

<b>Usage Guidelines</b>	You can use this command to re-authenticate a client without waiting for the configured number of seconds between re-authentication attempts (re-authperiod) and automatic re-authentication.
-------------------------	---

<b>Examples</b>	This example shows how to manually re-authenticate the device connected to a port:
-----------------	--

```
Switch# dot1x re-authenticate interface gigabitethernet0/1
```

# dot1x reauthentication

Use the **dot1x reauthentication** interface configuration command to enable periodic re-authentication of the client. Use the **no** form of this command to return to the default setting.

**dot1x reauthentication**

**no dot1x reauthentication**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Periodic re-authentication is disabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** You configure the amount of time between periodic re-authentication attempts by using the **dot1x timeout reauth-period** interface configuration command.

**Examples** This example shows how to disable periodic re-authentication of the client:

```
Switch(config-if)# no dot1x reauthentication
```

This example shows how to enable periodic re-authentication and to set the number of seconds between re-authentication attempts to 4000 seconds:

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000
```

You can verify your settings by entering the **show dot1x [interface interface-id]** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">dot1x timeout reauth-period</a>	Sets the number of seconds between re-authentication attempts.
	<a href="#">show dot1x [interface interface-id]</a>	Displays IEEE 802.1x status for the specified port.

# dot1x supplicant force-multicast

Use the **dot1x supplicant force-multicast** global configuration command 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 **no** form of this command to return to the default setting.

**dot1x supplicant force-multicast**

**no dot1x supplicant force-multicast**

**Syntax Description** This command has no arguments or keywords.

**Defaults** 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
	12.2(52)SE	This command was introduced.

**Usage Guidelines** Enable this command on the supplicant switch for Network Edge Access Topology (NEAT) to work in all host modes.

**Examples** This example shows how force a supplicant switch to send multicast EAPOL packets to authenticator switch:

```
Switch(config)# dot1x supplicant force-multicast
```

Related Commands	Command	Description
	<b>cisp enable</b>	Enable Client Information Signalling Protocol (CISP) on a switch so that it acts as an authenticator to a supplicant switch.
	<b>dot1x credentials</b>	Configure the 802.1x supplicant credentials on the port.
	<b>dot1x pae supplicant</b>	Configure an interface to act only as a supplicant.



# dot1x system-auth-control

Use the **dot1x system-auth-control** global configuration command to globally enable IEEE 802.1x. Use the **no** form of this command to return to the default setting.

**dot1x system-auth-control**

**no dot1x system-auth-control**

**Syntax Description** This command has no arguments or keywords.

**Defaults** IEEE 802.1x is disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** You must enable authentication, authorization, and accounting (AAA) and specify the authentication method list before globally enabling IEEE 802.1x. A method list describes the sequence and authentication methods to be queried to authenticate a user.

Before globally enabling IEEE 802.1x on a switch, remove the EtherChannel configuration from the interfaces on which IEEE 802.1x and EtherChannel are configured.

**Examples** This example shows how to globally enable IEEE 802.1x on a switch:

```
Switch(config)# dot1x system-auth-control
```

You can verify your settings by entering the **show dot1x [interface interface-id]** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">dot1x port-control</a>	Enables manual control of the authorization state of the port.
	<a href="#">show dot1x [interface interface-id]</a>	Displays IEEE 802.1x status for the specified port.

# dot1x test eapol-capable

Use the **dot1x test eapol-capable** privileged EXEC command 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.

**dot1x test eapol-capable** [*interface interface-id*]

<b>Syntax Description</b>	<b>interface</b> <i>interface-id</i> (Optional) Port to be queried.
---------------------------	---

<b>Defaults</b>	There is no default setting.
-----------------	------------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

<b>Usage Guidelines</b>	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 <b>no</b> form of this command.
-------------------------	---

<b>Examples</b>	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:
-----------------	---

```
switch# 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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>dot1x test timeout</b> <i>timeout</i>	Configures the timeout used to wait for EAPOL response to an IEEE 802.1x readiness query.

# dot1x test timeout

Use the **dot1x test timeout** global configuration command to configure the timeout used to wait for EAPOL response from a port being queried for IEEE 802.1x readiness.

**dot1x test timeout** *timeout*

<b>Syntax Description</b>	<i>timeout</i>	Time in seconds to wait for an EAPOL response. The range is from 1 to 65535 seconds.
---------------------------	----------------	--

<b>Defaults</b>	The default setting is 10 seconds.
-----------------	------------------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

<b>Usage Guidelines</b>	Use this command to configure the timeout used to wait for EAPOL response. There is not a <b>no</b> form of this command.
-------------------------	--

<b>Examples</b>	This example shows how to configure the switch to wait 27 seconds for an EAPOL response: Switch# <b>dot1x test timeout 27</b>
-----------------	--

You can verify the timeout configuration status by entering the **show run** privileged EXEC command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">dot1x test eapol-capable</a> [interface <i>interface-id</i> ]	Checks for IEEE 802.1x readiness on devices connected to all or to specified IEEE 802.1x-capable ports.

## dot1x timeout

Use the **dot1x timeout** interface configuration command to set IEEE 802.1x timers. Use the **no** form of this command to return to the default setting.

```
dot1x timeout { quiet-period seconds | reauth-period seconds | server-timeout seconds |
supp-timeout seconds | tx-period seconds }
```

```
no dot1x timeout { quiet-period | reauth-period | server-timeout | supp-timeout | tx-period }
```

### Syntax Description

<b>quiet-period</b> <i>seconds</i>	Number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The range is 1 to 65535.
<b>reauth-period</b> <i>seconds</i>	Number of seconds between re-authentication attempts. The range is 1 to 65535.
<b>server-timeout</b> <i>seconds</i>	Number of seconds that the switch waits for the retransmission of packets by the switch to the authentication server. The range is 1 to 65535. However, we recommend a minimum setting of 30.
<b>supp-timeout</b> <i>seconds</i>	Number of seconds that the switch waits for the retransmission of packets by the switch to the IEEE 802.1x client. The range is 30 to 65535.
<b>tx-period</b> <i>seconds</i>	Number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. The range is 1 to 65535.

### Defaults

These are the default settings:

**reauth-period** is 3600 seconds.

**quiet-period** is 60 seconds.

**tx-period** is 30 seconds.

**supp-timeout** is 30 seconds.

**server-timeout** is 30 seconds.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(44)EY	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.

### Examples

This example shows how to enable periodic re-authentication and to set 4000 as the number of seconds between re-authentication attempts:

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000
```

This example shows how to set 30 seconds as the quiet time on the switch:

```
Switch(config-if)# dot1x timeout quiet-period 30
```

This example shows how to set 45 seconds as the switch-to-authentication server retransmission time:

```
Switch(config)# dot1x timeout server-timeout 45
```

This example shows how to set 45 seconds as the switch-to-client retransmission time for the EAP request frame:

```
Switch(config-if)# dot1x timeout supp-timeout 45
```

This example shows how to set 60 as the number of seconds to wait for a response to an EAP-request/identity frame from the client before re-transmitting the request:

```
Switch(config-if)# dot1x timeout tx-period 60
```

You can verify your settings by entering the **show dot1x** privileged EXEC command.

### Related Commands

Command	Description
<a href="#">dot1x max-req</a>	Sets the maximum number of times that the switch sends an EAP-request/identity frame before restarting the authentication process.
<a href="#">dot1x reauthentication</a>	Enables periodic re-authentication of the client.
<a href="#">show dot1x</a>	Displays IEEE 802.1x status for all ports.

## dot1x violation-mode

Use the **dot1x violation-mode** interface configuration command 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.

**dot1x violation-mode {shutdown | restrict | protect}**

**no dot1x violation-mode**

Syntax Description	shutdown	Error disables the port or the virtual port on which a new unexpected MAC address occurs.
	<b>restrict</b>	Generates a syslog error when a violation error occurs.
	<b>protect</b>	Silently discards packets from any new MAC addresses. This is the default setting.

**Defaults** By default **dot1x violation-mode protect** is enabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Examples** This example shows how to configure an IEEE 802.1x-enabled port as error disabled and to shut down when a new device connects to the port:

```
Switch(config-if)# dot1x violation-mode shutdown
```

This example shows how to configure an IEEE 802.1x-enabled port to generate a system error message and change the port to restricted mode when a new device connects to the port:

```
Switch(config-if)# dot1x violation-mode restrict
```

This example shows how to configure an IEEE 802.1x-enabled port to ignore a new connected device when it is connected to the port:

```
Switch(config-if)# dot1x violation-mode protect
```

You can verify your settings by entering the **show dot1x [interface interface-id]** privileged EXEC command.

Related Commands	Command	Description
	<b>show dot1x [interface interface-id]</b>	Displays IEEE 802.1x status for the specified port.

# duplex

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

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

**no duplex**

## Syntax Description

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

## Defaults

The default is **auto** for Fast Ethernet and Gigabit Ethernet ports and for 1000BASE-T small form-factor pluggable (SFP) modules.

The default is **full** for 100BASE-FX MMF SFP modules.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

This command is only available when a 1000BASE-T SFP module or a 100BASE-FX MMF SFP module is in the SFP module slot. All other SFP modules operate only in full-duplex mode.

When a 1000BASE-T SFP module is in the SFP module slot, you can configure duplex mode to **auto** or **full**.

When a 100BASE-FX MMF SFP module is in the SFP module slot, you can configure duplex mode to **half** or **full**. Although the **auto** keyword is available, it puts the interface in half-duplex mode (the default) because the 100BASE-FX MMF SFP module does not support autonegotiation.

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

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 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.

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

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

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

**Caution**

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

**Note**

For guidelines on setting the switch speed and duplex parameters, see the software configuration guide for this release.

**Examples**

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

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

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

**Related Commands**

Command	Description
<a href="#">show interfaces</a>	Displays the interface settings on the switch.
<a href="#">speed</a>	Sets the speed on a 10/100 or 10/100/1000 Mbps interface.



# errdisable detect cause

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

```
errdisable detect cause {all | arp-inspection | dhcp-rate-limit | gbic-invalid | l2ptguard |
link-flap | loopback | pagp-flap | small-frame}
```

```
no errdisable detect cause {all | arp-inspection | dhcp-rate-limit | gbic-invalid | l2ptguard |
link-flap | pagp-flap | small-frame}
```



### Note

Although visible in the command line interface, **small-frame** keyword is not needed on the switch because the existing broadcast storm disable feature correctly handles small frames.

### Syntax Description

<b>all</b>	Enable error detection for all error-disable causes.
<b>arp-inspection</b>	Enable error detection for dynamic Address Resolution Protocol (ARP) inspection.
<b>dhcp-rate-limit</b>	Enable error detection for DHCP snooping.
<b>gbic-invalid</b>	Enable error detection for an invalid Gigabit Interface Converter (GBIC) module. <b>Note</b> This error refers to an invalid small form-factor pluggable (SFP) module.
<b>l2ptguard</b>	Enable error detection for a Layer 2 protocol-tunnel error-disabled cause.
<b>link-flap</b>	Enable error detection for link-state flapping.
<b>loopback</b>	Enable error detection for detected loopbacks.
<b>pagp-flap</b>	Enable error detection for the Port Aggregation Protocol (PAgP) flap error-disabled cause.
<b>small-frame</b>	This feature is not required on the switch.

### Defaults

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

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

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

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

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

### Examples

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

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

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

### Related Commands

Command	Description
<a href="#">show errdisable detect</a>	Displays errdisable detection information.
<a href="#">show interfaces status err-disabled</a>	Displays interface status or a list of interfaces in the error-disabled state.

## errdisable recovery

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

```
errdisable recovery {cause {all | arp-inspection | bpduguard | channel-misconfig |
dhcp-rate-limit | gbic-invalid | l2ptguard | link-flap | loopback | pagp-flap |
psecure-violation | security-violation | small-frame | udld unicast-flood | vmps} | {interval
interval}}
```

```
no errdisable recovery {cause {all | arp-inspection | bpduguard | channel-misconfig |
dhcp-rate-limit | gbic-invalid | l2ptguard | link-flap | loopback | pagp-flap |
psecure-violation | security-violation | small-frame | udld unicast-flood | vmps} | {interval
interval}}
```



### Note

Although visible in the command-line help strings, the **storm-control** and **unicast-flood** keywords are not supported. The **small-frame** keyword is not used because the broadcast-storm disable feature processes small frames

### Syntax Description

<b>cause</b>	Enable the error-disabled mechanism to recover from a specific cause.
<b>all</b>	Enable the timer to recover from all error-disabled causes.
<b>bpduguard</b>	Enable the timer to recover from the bridge protocol data unit (BPDU) guard error-disabled state.
<b>arp-inspection</b>	Enable the timer to recover from the Address Resolution Protocol (ARP) inspection error-disabled state.
<b>channel-misconfig</b>	Enable the timer to recover from the EtherChannel misconfiguration error-disabled state.
<b>dhcp-rate-limit</b>	Enable the timer to recover from the DHCP snooping error-disabled state.
<b>gbic-invalid</b>	Enable the timer to recover from an invalid Gigabit Interface Converter (GBIC) module error-disabled state. <b>Note</b> This error refers to an invalid small form-factor pluggable (SFP) error-disabled state.
<b>l2ptguard</b>	Enable the timer to recover from a Layer 2 protocol tunnel error-disabled state.
<b>link-flap</b>	Enable the timer to recover from the link-flap error-disabled state.
<b>loopback</b>	Enable the timer to recover from a loopback error-disabled state.
<b>pagp-flap</b>	Enable the timer to recover from the Port Aggregation Protocol (PAgP)-flap error-disabled state.
<b>psecure-violation</b>	Enable the timer to recover from a port security violation disabled state.
<b>security-violation</b>	Enable the timer to recover from an IEEE 802.1x-violation disabled state.
<b>small-frame</b>	This keyword is not used.
<b>udld</b>	Enable the timer to recover from the UniDirectional Link Detection (UDLD) error-disabled state.
<b>unicast-flood</b>	Enable the timer to recover from the unicast flood disable state.

<b>vmpls</b>	Enable the timer to recover from the VLAN Membership Policy Server (VMPS) error-disabled state.
<b>interval</b> <i>interval</i>	Specify the time to recover from the specified error-disabled state. The range is 30 to 86400 seconds. The same interval is applied to all causes. The default interval is 300 seconds.
<b>Note</b>	The error-disabled recovery timer is initialized at a random differential from the configured interval value. The difference between the actual timeout value and the configured value can be up to 15 percent of the configured interval.

**Defaults**

Recovery is disabled for all causes.  
The default recovery interval is 300 seconds.

**Command Modes**

Global configuration

**Command History**

Release	Modification
12.2(44)EY	This command was introduced.

**Usage Guidelines**

A cause (**all**, **bpduguard** and so forth) is defined as the reason that the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in error-disabled state, an operational state similar to link-down state. If you do not enable errdisable recovery for the cause, the interface stays in error-disabled state until you enter a **shutdown** and **no shutdown** interface configuration command. 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** then **no shutdown** commands to manually recover an interface from the error-disabled state

**Examples**

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

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

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

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

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

**Related Commands**

Command	Description
<a href="#">show errdisable recovery</a>	Displays errdisable recovery timer information.
<a href="#">show interfaces status err-disabled</a>	Displays interface status or a list of interfaces in error-disabled state.

# ethernet dot1ad

To configure an IEEE 802.1ad port, use the **ethernet dot1ad** interface configuration command. To disable an 802.1ad port, use the **no** form of the command.

```
ethernet dot1ad { nni | uni { c-port | s-port | c-port isolate | s-port isolate } }
```

```
no ethernet dot1ad
```

## Syntax Description

<b>nni</b>	Configures a network-network interface (NNI) port.
<b>uni</b>	Configures a user-network interface (UNI) port.
<b>c-port</b>	Configures a dot1ad UNI customer bridge port.
<b>s-port</b>	Configures a dot1ad UNI S-bridge port.
<b>c-port isolate</b>	Configures a split horizon by isolating a dot1ad C-UNI port.
<b>s-port isolate</b>	Configures a split horizon by isolating a dot1ad S-UNI port.

## Defaults

No 802.ad ports are configured.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(54)SE	This command was introduced.
12.2(55)SE	The <b>isolate</b> keywords were added.

## Usage Guidelines

The 802.1ad UNI port commands are typically used on the provider-edge switch ports interfacing with a customer device. For S-bridge UNI ports, you configure the customer device switch port as a trunk port and the S-bridge UNI on the interfacing PE device as an access port. The 802.1ad S-bridge UNI port provides an all-to-one bundling function for the set of customer C-VLANs in the provider network.

The 802.1ad C-bridge UNI ports provide selective bundling as well as all-to-one bundling capabilities for customer VLANs.

You should configure an 802.1ad NNI on all the interconnecting trunk links in the 802.1ad provider cloud to achieve end-to-end Layer 2 protocol tunneling.

You cannot configure a port as an isolated C-UNI or S-UNI port if the port is already configured as an 802.1ad port type. However, you can use the **ethernet dot1ad** interface command to change an isolated dot1ad port to a nonisolated S-UNI or C-UNI port.

An S-UNI or isolated S-UNI port must be an access port. A C-UNI or isolated C-UNI port can be an access port or a trunk port.

■ ethernet dot1ad

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>l2protocol</b>	Configures a port to process or forward Layer 2 BPDUs.
<b>show ethernet dot1ad</b>	Displays 802.1ad port configuration on the switch.

# ethernet evc

Use the **ethernet evc** global configuration command to define an Ethernet virtual connection (EVC) and to enter EVC configuration mode. Use the **no** form of this command to delete the EVC.

**ethernet evc** *evc-id*

**no ethernet evc** *evc-id*

Syntax Description	<i>evc-id</i>	The EVC identifier. This can be a string of from 1 to 100 characters.
--------------------	---------------	---

Defaults	No EVCs are defined.
----------	----------------------

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** After you enter the **ethernet evc** *evc-id* command, the switch enters EVC configuration mode, and these configuration commands are available:

- **default**: sets the EVC to its default states.
- **exit**: exits EVC configuration mode and returns to global configuration mode.
- **no**: negates a command or returns a command to its default setting.
- **oam protocol cfm svlan**: configures the Ethernet operation, administration, and maintenance (OAM) protocol as IEEE 802.1ag Connectivity Fault Management (CFM) and sets parameters. See the [oam protocol cfm svlan](#) command.
- **uni count**: configures a UNI count for the EVC. See the [uni count](#) command.

**Examples** This example shows how to define an EVC and to enter EVC configuration mode:

```
Switch(config)# ethernet evc test1
Switch(config-vc)#
```

Related Commands	Command	Description
	<a href="#">service instance</a> <i>id</i> <b>ethernet</b> <i>evc-id</i>	Configures an Ethernet service instance and attaches an EVC to it.
	<a href="#">show ethernet service evc</a>	Displays information about configured EVCs.

# ethernet lmi

Use the **ethernet lmi** global configuration command to configure enable Ethernet Local Management Interface (E-LMI) and to configure the switch as a provider-edge (PE) or customer-edge (CE) device. Use the **no** form of this command to disable E-LMI globally or to disable E-LMI CE.

**ethernet lmi** {ce | global}

**no ethernet lmi** {ce | global}

## Syntax Description

<b>ce</b>	Enable the switch as an E-LMI CE device.  <b>Note</b> Ethernet LMI is disabled by default. You must enable it globally or on an interface in addition to enabling it in CE mode.
<b>global</b>	Enable E-LMI globally on the switch. By default, the switch is a PE device.

## Defaults

Ethernet LMI is disabled. When enabled with the global keyword, by default the switch is a PR device.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

Use **ethernet lmi global** command to enable E-LMI globally. Use **ethernet lmi ce** command to enable the switch as E-LMI CE device.

Ethernet LMI is disabled by default on an interface and must be explicitly enabled by entering the **ethernet lmi interface** interface configuration command. The **ethernet lmi global** command enables Ethernet LMI in PE mode on all interfaces for an entire device. The benefit of this command is that you can enable Ethernet LMI on all interfaces with one command instead of enabling Ethernet LMI separately on each interface. To enable the interface in CE mode, you must also enter the **ethernet lmi ce** global configuration command.

To disable Ethernet LMI on a specific interface after you have entered the **ethernet lmi global** command, enter the **no ethernet lmi interface** interface configuration command.

The sequence in which you enter the **ethernet lmi interface** interface configuration and **ethernet lmi global** global configuration commands is important. The latest command entered overrides the prior command entered.



### Note

For information about the **ethernet lmi** interface configuration command, see the *Cisco IOS Carrier Ethernet Command Reference* at this URL:

[http://www.cisco.com/en/US/docs/ios/cether/command/reference/ce\\_book.html](http://www.cisco.com/en/US/docs/ios/cether/command/reference/ce_book.html)



To enable the switch as an Ethernet LMI CE device, you must enter both the **ethernet lmi global** and **ethernet lmi ce** commands. By default Ethernet LMI is disabled, and, when enabled the switch is in provider-edge mode unless you also enter the **ethernet lmi ce** command.

When the switch is configured as an Ethernet LMI CE device, these interface configuration commands and keywords are visible, but not supported:

- **service instance**
- **ethernet uni**
- **ethernet lmi t392**

---

**Examples**

This example shows how to configure the switch as an Ethernet LMI CE device:

```
Switch(config)# ethernet lmi global
Switch(config)# ethernet lmi ce
```

---

**Related Commands**

Command	Description
<b>ethernet lmi interface configuration command</b>	Enables Ethernet LMI for a user-network interface.

## ethernet lmi ce-vlan map

Use the **ethernet lmi ce-vlan map** Ethernet service configuration command to configure Ethernet Local Management Interface (E-LMI) parameters. Use the **no** form of this command to remove the configuration.

**ethernet lmi ce-vlan map** {*vlan-id* | **any** | **default** | **untagged**}

**no ethernet lmi ce-vlan map** {*vlan-id* | **any** | **default** | **untagged**}

### Syntax Description

<i>vlan-id</i>	Enter the customer VLAN ID or VLAN IDs to map to. You can enter a single VLAN ID (the range is 1 to 4094), a range of VLAN IDs separated by a hyphen, or a series of VLAN IDs separated by commas.
<b>any</b>	Map all VLANs (untagged and VLANs 1 to 4094).
<b>default</b>	Map to the default service instance. You can use the <b>default</b> keyword only if you have already mapped the service instance to a VLAN or a group of VLANs.
<b>untagged</b>	Map only untagged VLANs.

### Defaults

No E-LMI mapping parameters are defined.

### Command Modes

Ethernet service configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

Use this command to configure an E-LMI customer VLAN-to-EVC map for a particular user-network interface (UNI).

On an ME-3400E interface configured for VLAN mapping, use the customer VLAN ID (C-VLAN) value when entering the **ethernet lmi ce-vlan map** *vlan-id* service instance configuration mode command. Do not use the service-provider VLAN ID (S-VLAN).

E-LMI mapping parameters are related to the bundling characteristics set by entering the **ethernet uni** {**bundle** [**all-to-one**] | **multiplex**} interface configuration command.

- Using the default UNI attribute (bundling and multiplexing) supports multiple EVCs and multiple VLANs.
- Entering the **ethernet uni bundle** command supports only one EVC with one or more VLANs.
- Entering the **ethernet uni bundle all-to-one** command supports multiple VLANs but only one EVC. If you use the **ethernet lmi ce-vlan map any** Ethernet service configuration command, you must first configure **all-to-one** bundling on the interface.
- Entering the **ethernet uni multiplex** command supports multiple EVCs with only one VLAN per EVC.

---

**Examples**

This example shows how to configure an E-LMI customer VLAN-to-EVC map to map EVC *test* to customer VLAN 101 in service instance 333 on the interface:

```
Switch(config-if)# service instance 333 ethernet test  
Switch(config-if-srv)# ethernet lmi ce-vlan map 101
```

---

**Related Commands**

Command	Description
<a href="#">service instance <i>id</i></a> <a href="#">ethernet</a>	Defines an Ethernet service instance and enters Ethernet service configuration mode.
<a href="#">show ethernet service instance</a>	Displays information about configured Ethernet service instances.

---

## ethernet loopback (interface configuration)

Use the **ethernet loopback facility** interface configuration command to configure per-port loopbacks for testing connectivity across multiple switches. Use the **ethernet loopback terminal** interface configuration command to test quality of service (QoS). Use the **no** form of this command to remove the configuration.

**ethernet loopback facility** [**vlan** *vlan-list*] [**mac-address** {**swap** | **copy**}] [**timeout** {*seconds* | **none**}] **supported**

**ethernet loopback terminal** [**mac-address** {**swap** | **copy**}] [**timeout** {*seconds* | **none**}] **supported**

**no ethernet loopback**

Syntax Description		
<b>facility</b>		Configure a facility loopback for connectivity testing.
<b>vlan</b> <i>vlan-list</i>		Configure VLAN loopback for nondisruptive loopback testing.
<b>terminal</b>		Configure a terminal loopback for QoS testing.
<b>mac-address swap</b>		Configure the switch to swap the MAC source and destination addresses for the loopback action.
<b>mac-address copy</b>		Configure the switch to copy the MAC source and destination addresses for the loopback action.
<b>timeout</b> <i>seconds</i>		Configure a loopback timeout period in seconds. The range is from 5 to 300 seconds. The default is 60 seconds.
<b>timeout none</b>		Configure the loop back to not timeout.
<b>supported</b>		Specify that the configured loopback is supported.

### Defaults

No loopbacks are configured. If no **mac-address** option is configured, the default is to copy the source and destination addresses.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.
12.2(50)SE	The <b>vlan</b> and <b>terminal</b> keywords were added.

### Usage Guidelines

You can configure Ethernet loopback only on physical ports, not on VLANs or port channels.

A facility loopback puts the port into a state where the link is up, but the line protocol is down for regular traffic. The switch loops back all received traffic.

When you configure VLAN loopback by entering the **vlan** *vlan-list* keywords, the other VLANs on the port continue to be switched normally, allowing non-disruptive loopback testing.

The loopback ends after a port event, such as a port shutdown or a change from a switchport to a routed port.

For a terminal loopback, the software sees the port as up, but the link is down, and no packets are sent. Any configuration changes on the port immediately affect the traffic being looped back.

You can configure one loopback per port, and a maximum of two loopbacks per switch. You can configure only one terminal loopback per switch. Therefore, a switch could have one facility loopback and one terminal loopback or two facility loopbacks.

Ethernet loopback interactions with other features:

- You cannot configure SPAN and loopback on a switch at the same time. If you try to configure SPAN on any port while loopback is configured on any port, you receive an error message.
- The port loopback function shares hardware resources with the VLAN-mapping feature. If not enough TCAM resources are available because of VLAN-mapping configuration, when you attempt to configure loopback, you receive an error message, and the configuration is not allowed.
- If loopback is active on a port, you cannot add that port to a Flex Link pair or to an Ether Channel.

After you have configured Ethernet loopback, you enter the **ethernet loopback start** *interface-id* privileged EXEC command to begin the loopback. To stop loopback, enter the **ethernet loopback stop** *{interface-id | all}* command.

## Examples

This example shows how to configure an Ethernet loopback to swap the MAC source and destination addresses, to time out after 30 seconds, to start the loopback process, and to verify the configuration. You must confirm the action before configuring.

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# ethernet loopback facility mac-address swap timeout 30 supported
Switch(config-if)# end
Switch# ethernet loopback start gigabitethernet 0/1
This is an intrusive loopback.
Therefore, while you test Ethernet connectivity,
you will be unable to pass traffic across that link.
Proceed with Local Loopback? [confirm]
```

```
Switch# show ethernet loopback
=====
Loopback Session 0 : Interface GI0/1
Direction          : facility
Type               : port
Status             : active
MAC Mode           : swap
Time out           : 30
Time remaining     : 25 seconds
```

This example shows how to also configure a nondisruptive loopback on a second interface:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# ethernet loop facility mac-address swap timeout none supported
Switch(config-if)# exit
Switch(config-if)# interface fastethernet0/2
Switch(config-if)# ethernet loop facility vlan 3 mac-address copy timeout 100 supported
switch(config-if)# switch mode trunk
Switch(config-if)# exit
switch(config)# vlan 3
switch(config-vlan)# end
```

```
Switch# show ethernet loopback
=====
Loopback Session 0 : Interface Fa0/1
Direction          : facility
Type               : port
Status             : configured
MAC Mode          : swap
Time out          : none
=====
Loopback Session 1 : Interface Fa0/2
Direction          : facility
Type               : vlan
Status            : configured
MAC Mode          : copy
Vlan              : 3
Time out          : 100
```

This example shows how to remove Ethernet loopback facility configuration on two interfaces and to configure Ethernet terminal loopback on an interface.

```
Switch(config)# interface fastethernet 0/1
switch(config-if)# no ethernet loopback
switch(config-if)# interface fastethernet 0/2
switch(config-if)# no ethernet loopback
switch(config-if)# exit
switch(config)# default interface range fastethernet 0/1-2
switch(config)# interface fastethernet 0/1
switch(config-if)# ethernet loop terminal mad-address swap timeout 300 supported
switch(config-if)# end
```

```
Switch# show ethernet loopback
=====
Loopback Session 0 : Interface Fa0/1
Direction          : terminal
Type               : port
Status             : configured
MAC Mode          : swap
Time out          : 300
```

#### Related Commands

Command	Description
<a href="#">ethernet loopback (privileged EXEC)</a>	Starts or stops an Ethernet loopback operation on an interface.
<a href="#">show ethernet loopback</a>	Displays the Ethernet loopbacks configured on the switch or the specified interface.

# ethernet loopback (privileged EXEC)

Use the **ethernet loopback** privileged EXEC command to start or stop an Ethernet loopback function on an interface.

```
ethernet loopback {start interface-id | stop {interface-id | all}}
```

## Syntax Description

<b>start</b>	Start the Ethernet loopback operation configured on the interface.
<b>stop</b>	Stop the Ethernet loopback operation.
<i>interface-id</i>	Specify the interface on which to start or stop the loopback operation.
<b>all</b>	Stop all Ethernet loopback operations on the switch. This keyword is available only after the <b>stop</b> keyword.

## Defaults

There is no default.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

Before starting or stopping an Ethernet loopback operation, you must configure it on an interface by entering the **ethernet loopback** interface configuration command. When you start loopback, you see a warning message.

You can configure Ethernet loopback and enter the **ethernet loopback start** or **ethernet loopback stop** command only for physical ports, not for VLANs or port channels.

You cannot start VLAN loopback on nontrunk interfaces. You cannot start terminal loopback on routed interfaces.

You can configure only one loopback per port and a maximum of two loopbacks per switch. You can configure only one terminal loopback per switch.

## Examples

This example shows how to start a facility port loopback process, to verify it, and then to stop it:

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# ethernet loopback facility mac-address swap timeout 30 supported
Switch(config-if)# end
Switch# ethernet loopback start gigabitethernet 0/1
This is an intrusive loopback.
Therefore, while you test Ethernet connectivity,
you will be unable to pass traffic across that link.
Proceed with Local Loopback? [confirm]
```

```

Switch# show ethernet loopback
=====
Loopback Session 0 : Interface Gi0/1
Direction          : facility
Type               : port
Status             : active
MAC Mode           : swap
Time out           : 30
Time remaining     : 25 seconds

Switch# ethernet loop stop all

Dec 4 11:18:44.083: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up

Switch# show ethernet loopback
=====
Loopback Session 0 : Interface Gi0/1
Direction          : facility
Type               : port
Status             : configured
MAC Mode           : swap
Time out           : 30

```

This example shows how to start a VLAN non-intrusive loopback process:

```

Switch# ethernet loop start fastethernet 0/2
This is a non-intrusive loopback.
Therefore, while you test Ethernet connectivity on vlan 3, you will be unable to pass
traffic across it, however, other vlans will be unaffected.
Proceed with Local Loopback? [confirm]

Switch# show ethernet loopback
=====
Loopback Session 1 : Interface Fa0/2
Direction          : facility
Type               : vlan
Status             : active
MAC Mode           : copy
Vlan               : 3
Time out           : 100
Time remaining     : 94 seconds

```

#### Related Commands

Command	Description
<a href="#">ethernet loopback (interface configuration)</a>	Configures an Ethernet loopback operation on an interface.
<a href="#">show ethernet loopback</a>	Displays the Ethernet loopbacks configured on the switch or the specified interface.



# ethernet oam remote-failure

Use the **ethernet oam remote-failure** interface configuration or configuration template command to configure Ethernet operations, maintenance, and administration (EOM) remote failure indication. Use the **no** form of this command to remove the configuration.

```
ethernet oam remote-failure {critical-event | dying-gasp | link-fault} action
error-disable-interface
```

```
no ethernet oam remote-failure {critical-event | dying-gasp | link-fault} action
```

Syntax Description		
<b>critical-event</b>		Configure the switch to put an interface in error-disabled mode when an unspecified critical event has occurred.
<b>dying-gasp</b>		Configure the switch to put an interface in error-disabled mode when an unrecoverable condition has occurred.
<b>link-fault</b>		Configure the switch to put an interface in error-disabled mode when the receiver detects a loss of power.

## Defaults

Configuration template  
Interface configuration

## Command Modes

Ethernet service configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

You can apply this command to an Ethernet OAM template and to an interface. The interface configuration takes precedence over template configuration. To enter OAM template configuration mode, use the **template** template-name global configuration command.

The Cisco ME switch does not generate Link Fault or Critical Event OAM PDUs. However, if these PDUs are received from a link partner, they are processed. The switch supports generating and receiving Dying Gasp OAM PDUs when Ethernet OAM is disabled, the interface is shut down, the interface enters the error-disabled state, or the switch is reloading. The switch can also generate and receive Dying Gasp PDUs based on loss of power. The PDU includes a reason code to indicate why it was sent.

You can configure an error-disable action to occur if the remote link goes down, if the remote device is disabled, or if the remote device disables Ethernet OAM on the interface.

For complete command and configuration information for the Ethernet OAM protocol, see the *Cisco IOS Carrier Ethernet Configuration Guide* at:

[http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/12\\_2sr/ce\\_12\\_2sr\\_book.html](http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/12_2sr/ce_12_2sr_book.html)

For information about other CFM and Ethernet OAM commands, see the *Cisco IOS Carrier Ethernet Command Reference* at:

[http://www.cisco.com/en/US/docs/ios/cether/command/reference/ce\\_book.html](http://www.cisco.com/en/US/docs/ios/cether/command/reference/ce_book.html)

**Examples**

This example shows how to configure an Ethernet OAM template for remote-failure indication when an unrecoverable error has occurred and how to apply it to an interface:

```
Switch(config)# template oam1
Switch(config-template)# ethernet oam remote-failure dying-gasp action error-disable interface
Switch(config-template)# exit
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# source template oam1
Switch(config-if)# exit
```

This example shows how to configure an Ethernet OAM remote-failure indication on one interface for unrecoverable errors:

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# ethernet oam remote-failure dying-gasp action error-disable interface
Switch(config-if)# exit
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show ethernet oam status [interface interface-id]</b>	Displays configured Ethernet OAM remote failure conditions on all interfaces or on the specified interface.

# ethernet uni

Use the **ethernet uni** interface configuration command to set UNI bundling attributes. Use the **no** form of this command to return to the default bundling configuration.

**ethernet uni { bundle [all-to-one] | multiplex }**

**no ethernet uni { bundle | multiplex }**

## Syntax Description

<b>bundle</b>	Configure the UNI to support bundling without multiplexing. This service supports only one Ethernet virtual connection (EVC) at the UNI with one or multiple customer edge (CE)-VLAN IDs mapped to the EVC.
<b>all-to-one</b>	(Optional) Configure the UNI to support bundling with a single EVC at the UNI and all CE VLANs mapped to that EVC.
<b>multiplex</b>	Configure the UNI to support multiplexing without bundling. The UNI can have one or more EVCs with a single CE-VLAN ID mapped to each EVC.

## Defaults

If bundling or multiplexing attributes are not configured, the default is bundling with multiplexing. The UNI then has one or more EVCs with one or more CE VLANs mapped to each EVC.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The UNI attributes determine the functionality that the interface has regarding bundling VLANs, multiplexing EVCs, and the combination of these.

If you want both bundling and multiplexing services for a UNI, you do not need to configure bundling or multiplexing. If you want only bundling, or only multiplexing, you need to configure it appropriately.

When you configure, change, or remove a UNI service type, the EVC and CE-VLAN ID configurations are checked to ensure that the configurations and the UNI service types match. If the configurations do not match, the command is rejected.

If you intend to use the **ethernet lmi ce-vlan map any** service configuration command, you must first configure **all-to-one** bundling on the interface. See the [ethernet lmi ce-vlan map](#) section for more information.

## Examples

This example shows how to configure bundling without multiplexing:

```
Switch(config-if)# ethernet uni bundle
```

To verify UNI service type, enter the **show ethernet service interface detail** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">show ethernet service interface</a>	Displays information about Ethernet service instances on an interface, including service type.

# ethernet uni id

Use the **ethernet uni** interface configuration command to create an Ethernet user-network interface (UNI) ID. Use the **no** form of this command to remove the UNI ID.

**ethernet uni id** *name*

**no ethernet uni id**

## Syntax Description

<i>name</i>	Identify an Ethernet UNI ID. The name should be unique for all UNIs that are part of a given service instance and can be up to 64 characters in length.
-------------	---

## Defaults

No UNI IDs are created.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

When you configure a UNI ID on a port, that ID is used as the default name for all maintenance end points (MEPs) configured on the port.

You must enter the **ethernet uni id** *name* command on all ports that are directly connected to customer-edge (CE) devices. If the specified ID is not unique on the device, an error message appears.

## Examples

This example shows how to identify a unique UNI:

```
Switch(config-if)# ethernet uni id test2
```

## Related Commands

Command	Description
<a href="#">show ethernet service interface</a>	Displays information about Ethernet service instances on an interface, including service type.

## exceed-action

Use the **exceed-action** policy-map class police configuration command to set multiple actions for a policy-map class for packets with a rate between the committed information rate (CIR) or peak information rate (PIR) conform rate and the conform rate plus the exceed burst. Use the **no** form of this command to cancel the action or to return to the default action.

```
exceed-action { drop | set-cos-transmit { new-cos-value | [cos | dscp | precedence] [table
table-map name]} | set-dscp-transmit { new-dscp-value | [cos | dscp | precedence] [table
table-map name]} | set-prec-transmit { new-precedence-value | [cos | dscp | precedence]
[table table-map name]} | set-qos-transmit qos-group-value | transmit }
```

```
no exceed-action { drop | set-cos-transmit { new-cos-value | [cos | dscp | precedence] [table
table-map name]} | set-dscp-transmit { new-dscp-value | [cos | dscp | precedence] [table
table-map name]} | set-prec-transmit { new-precedence-value | [cos | dscp | precedence]
[table table-map name]} | set-qos-transmit qos-group-value | transmit }
```

Syntax Description	
<b>drop</b>	Drop the packet.
<b>set-cos-transmit</b> <i>new-cos-value</i>	Set a new class of service (CoS) value for the packet and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new CoS value is 0 to 7.
<b>set-dscp-transmit</b> <i>new-dscp-value</i>	Set a new Differentiated Services Code Point (DSCP) value for the packet and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new DSCP value is 0 to 63.
<b>set-prec-transmit</b> <i>new-precedence-value</i>	Set a new IP precedence value for the packet and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new IP precedence value is 0 to 7.
<b>set-qos-transmit</b> <i>qos-group-value</i>	Set a new quality of service (QoS) group value for the packet and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new QoS value is 0 to 99.
<b>cos</b>	(Optional) Set the packet marking specified in the preceding keyword based on the CoS value of the incoming packet, and send the packet. This specifies the <i>from-type</i> of the enhanced packet-marking action.
<b>dscp</b>	(Optional) Set the packet marking specified in the preceding keyword based on the DSCP value of the incoming packet, and send the packet. This specifies the <i>from-type</i> of the enhanced packet-marking action.
<b>precedence</b>	(Optional) Set the packet marking specified in the preceding keyword based on the IP precedence value of the incoming packet, and send the packet. This specifies the <i>from-type</i> of the enhanced packet-marking action.
<b>table</b> <i>table-map name</i>	(Optional) Used in conjunction with the preceding <i>from-type</i> keyword. Specify the table map to be used for the enhanced packet marking. The <i>to-type</i> of the action is marked based on the <i>from-type</i> parameter of the action using this table map.
<b>transmit</b>	(Optional) Send the packet unmodified.

### Defaults

The default action is to drop the packet.

**Command Modes** Policy-map class police configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** You configure exceed actions for packets when the packet rate is between the configured conform rate and the conform rate plus the exceed burst.

If the conform action is set to **drop**, the exceed and violate actions are automatically set to **drop**. If the exceed action is set to **drop**, the violate action is automatically set to **drop**.

You can configure exceed-action to send the packet unmodified, mark using explicit values, and use all combinations of enhanced packet marking. Enhanced packet marking provides the ability to modify a QoS marking based on any incoming QoS marking and table maps. The switch also supports the ability to mark multiple QoS parameters for the same class and to simultaneously configure conform-action, exceed-action, and violate-action marking.

Access policy-map class police configuration mode by entering the **police** policy-map class command. See the **police** command for more information.

You can use this command to set one or more exceed actions for a traffic class.

**Examples** This example shows how configure multiple actions in a policy map that sets an information rate of 23000 bits per second (b/s) and a burst rate of 10000 bps:

```
Switch(config)# policy-map map1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police 23000 10000
Switch(config-pmap-c-police)# conform-action transmit
Switch(config-pmap-c-police)# exceed-action set-prec-transmit prec table
policed-prec-table-map-name
Switch(config-pmap-c-police)# exit
```

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

Related Commands	Command	Description
	<b>class</b>	Defines a traffic classification match criteria for the specified class-map name.
	<b>conform-action</b>	Defines the action to take on traffic that conforms to the CIR.
	<b>police</b>	Defines a policer for classified traffic.
	<b>policy-map</b>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
	<b>show policy-map</b>	Displays QoS policy maps.
	<b>violate-action</b>	Defines the action to take on traffic with a rate greater than the conform rate plus the exceed burst.

# flowcontrol

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

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

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



## Note

The Cisco ME switch can only receive pause frames.

## Syntax Description

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

## Defaults

The default is **flowcontrol receive off**.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The switch does not support sending flow-control pause frames. If the port is a user network interface (UNI) or enhanced network interface (ENI), you must use the **no shutdown** interface configuration command to enable it before using the **flowcontrol** command. UNIs and ENIs are disabled by default. Network node interfaces (NNIs) are enabled by default.

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

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

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



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

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

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

### Examples

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

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

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

### Related Commands

Command	Description
<a href="#">show interfaces</a>	Displays the interface settings on the switch, including input and output flow control.

# hw-module module logging onboard

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

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

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

Syntax Description	
<i>slot-number</i>	(Optional) The slot number is always 1 and is not relevant for the ME-3400E.
<b>message level</b> <i>level</i>	(Optional) Specify the severity of the hardware-related messages that are stored in the flash memory. The range is from 1 to 7 with 1 being the most severe.

**Defaults** OBFL is enabled, and all messages appear.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines**

We recommend that you keep OBFL enabled and do not clear the data stored in the flash memory. To ensure that the time stamps in the OBFL data logs are accurate, 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.

The optional slot number is always 1. Entering the **hw-module module** [*slot-number*] **logging onboard** [**message level** *level*] command has the same result as entering the **hw-module module logging onboard** [**message level** *level*] command.

**Examples** This example shows how to enable OBFL on a switch stack and to specify that all the hardware-related messages are stored in the flash memory:

```
Switch(config)# hw-module module logging onboard
```

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

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

You can verify your settings by entering the [show logging onboard](#) privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">clear logging onboard</a>	Removes the OBFL data in the flash memory.
<a href="#">show logging onboard</a>	Displays OBFL information.

# interface port-channel

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

**interface port-channel** *port-channel-number*

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

---

<b>Syntax Description</b>	<i>port-channel-number</i> Port-channel number. The range is 1 to 48.
---------------------------	---

---



---

<b>Defaults</b>	No port-channel logical interfaces are defined.
-----------------	---

---



---

<b>Command Modes</b>	Global configuration
----------------------	----------------------

---



---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

---



---

**Usage Guidelines**

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

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 only on the physical port and not on the port-channel interface.



**Note** CDP is available only on network node interfaces (NNIs) and enhanced network interfaces (ENIs).

- 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.

### Examples

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

```
Switch(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 Commands

Command	Description
<b>channel-group</b>	Assigns an Ethernet port to an EtherChannel group.
<b>show etherchannel</b>	Displays EtherChannel information for a channel.
<b>show running-config</b>	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: <a href="http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html">http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html</a> Select the <b>Cisco IOS Commands Master List, Release 12.2</b> to navigate to the command.

# interface range

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

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

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

## Syntax Description

<i>port-range</i>	Port range. For a list of valid values for <i>port-range</i> , see the “Usage Guidelines” section.
<b>macro name</b>	Specify the name of a macro.

## Defaults

This command has no default setting.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

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

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

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

You can enter the interface range in two ways:

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

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

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

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

- **gigabitethernet** *module*{*first port*} - {*last port*}, where *module* is always 0  
For physical interfaces:
  - *module* is always 0
  - the range is *type 0/number - number* (for example, **gigabitethernet0/1 - 2**)
- **port-channel** *port-channel-number* - *port-channel-number*, where *port-channel-number* is from 1 to 48

**Note**

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

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

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

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

```
interface range fastethernet0/1 - 2, gigabitethernet0/1 - 2
```

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

A single interface can also be specified in *port-range* (this would make the command similar to the **interface** *interface-id* global configuration command).

**Note**

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

**Examples**

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

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

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

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

**Related Commands**

Command	Description
<b>define interface-range</b>	Creates an interface range macro.
<b>show running-config</b>	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: <a href="http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html">http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html</a> Select the <b>Cisco IOS Commands Master List, Release 12.2</b> to navigate to the command.

# interface vlan

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

**interface vlan** *vlan-id*

**no interface vlan** *vlan-id*

## Syntax Description

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

## Defaults

The default VLAN interface is VLAN 1.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

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



### Note

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

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



### Note

You cannot delete the VLAN 1 interface.

You can reinstate a deleted SVI by entering the **interface vlan** *vlan-id* command for the deleted interface. The interface comes back up, but much of the previous configuration will be gone.

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

## Examples

This example shows how to create VLAN ID 23 and enter interface configuration mode:

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



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

Related Commands	Command	Description
	<b>show interfaces</b> <b>vlan</b> <i>vlan-id</i>	Displays the administrative and operational status of all interfaces or the specified VLAN.

## ip access-group

Use the **ip access-group** interface configuration command to control access to a Layer 2 or Layer 3 interface. Use the **no** form of this command to remove all access groups or the specified access group from the interface. If the switch is running the metro IP access image, you can also control access to Layer 3 interfaces.

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

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

Syntax Description		
<i>access-list-number</i>	The number of the IP access control list (ACL). The range is 1 to 199 or 1300 to 2699.	
<i>name</i>	The name of an IP ACL, specified in the <b>ip access-list</b> global configuration command.	
<b>in</b>	Specify filtering on inbound packets.	
<b>out</b>	Specify filtering on outbound packets. This keyword is valid only on Layer 3 interfaces.	

**Defaults** No access list is applied to the interface.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

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

The switch must be running the metro IP access image for Layer 3 support.

You can use this command to apply an access list to a Layer 2 interface (port ACL) or Layer 3 interface. However, note these limitations for port ACLs:

- You can only apply ACLs in the inbound direction; the **out** keyword is not supported for Layer 2 interfaces.
- You can only apply one IP ACL and one MAC ACL per interface.
- Port ACLs do not support logging; if the **log** keyword is specified in the IP ACL, it is ignored.
- An IP ACL applied to a Layer 2 interface only filters IP packets. To filter non-IP packets, use the **mac access-group** interface configuration command with MAC extended ACLs.

You can use router ACLs, input port ACLs, and VLAN maps on the same switch. However, a port ACL always takes precedence. When both an input port ACL and a VLAN map are applied, incoming packets received on ports with the port ACL applied are filtered by the port ACL. Other packets are filtered by the VLAN map.

- When an input port ACL is applied to an interface and a VLAN map is applied to a VLAN that the interface is a member of, incoming packets received on ports with the ACL applied are filtered by the port ACL. Other packets are filtered by the VLAN map.
- When an input router ACL and input port ACLs exist in an switch virtual interface (SVI), incoming packets received on ports to which a port ACL is applied are filtered by the port ACL. Incoming routed IP packets received on other ports are filtered by the router ACL. Other packets are not filtered.
- When an output router ACL and input port ACLs exist in an SVI, incoming packets received on the ports to which a port ACL is applied are filtered by the port ACL. Outgoing routed IP packets are filtered by the router ACL. Other packets are not filtered.
- When a VLAN map, input router ACLs, and input port ACLs exist in an SVI, incoming packets received on the ports to which a port ACL is applied are only filtered by the port ACL. Incoming routed IP packets received on other ports are filtered by both the VLAN map and the router ACL. Other packets are filtered only by the VLAN map.
- When a VLAN map, output router ACLs, and input port ACLs exist in an SVI, incoming packets received on the ports to which a port ACL is applied are only filtered by the port ACL. Outgoing routed IP packets are filtered by both the VLAN map and the router ACL. Other packets are filtered only by the VLAN map.

You can apply IP ACLs to both outbound or inbound Layer 3 interfaces.

A Layer 3 interface can have one IP ACL applied in each direction.

You can configure only one VLAN map and one router ACL in each direction (input/output) on a VLAN interface.

For standard inbound access lists, after the switch receives a packet, it checks the source address of the packet against the access list. IP extended access lists can optionally check other fields in the packet, such as the destination IP address, protocol type, or port numbers. If the access list permits the packet, the switch continues to process the packet. If the access list denies the packet, the switch discards the packet. If the access list has been applied to a Layer 3 interface, discarding a packet (by default) causes the generation of an Internet Control Message Protocol (ICMP) Host Unreachable message. ICMP Host Unreachable messages are not generated for packets discarded on a Layer 2 interface.

For standard outbound access lists, after receiving a packet and sending it to a controlled interface, the switch checks the packet against the access list. If the access list permits the packet, the switch sends the packet. If the access list denies the packet, the switch discards the packet and, by default, generates an ICMP Host Unreachable message.

If the specified access list does not exist, all packets are passed.

---

### Examples

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

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

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

Related Commands	Command	Description
	access list	Configures a numbered ACL.
	ip access-list	Configures a named ACL.
	<a href="#">show access-lists</a>	Displays ACLs configured on the switch.
	show ip access-lists	Displays IP ACLs configured on the switch.
	show ip interface	Displays information about interface status and configuration.

# ip address

Use the **ip address** interface configuration command to set an IP address for the Layer 2 switch or to set an IP address for each switch virtual interface (SVI) or routed port on the Layer 3 switch. Use the **no** form of this command to remove an IP address or to disable IP processing.

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

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



## Note

You can configure routed ports and SVIs only when the switch is running the metro IP access image.

## Syntax Description

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

## Defaults

No IP address is defined.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

If you remove the switch IP address through a Telnet session, your connection to the switch will be lost. Hosts can find subnet masks using the Internet Control Message Protocol (ICMP) Mask Request message. Routers respond to this request with an ICMP Mask Reply message.

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

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



## Note

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

When you are routing Open Shortest Path First (OSPF), ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses.

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

A Layer 3 switch can have an IP address assigned to each routed port and SVI. The number of routed ports and SVIs that you can configure is not limited by software; however, the interrelationship between this number 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. For more information, see the **sdm prefer** command.

### Examples

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

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

This example shows how to configure the IP address for a Layer 3 port on the switch:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.20.128.2 255.255.255.0
```

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

### Related Commands

Command	Description
<b>show running-config</b>	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: <a href="http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html">http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html</a> Select the <b>Cisco IOS Commands Master List, Release 12.2</b> to navigate to the command.

## ip arp inspection filter vlan

Use the **ip arp inspection filter vlan** global configuration command to permit or deny Address Resolution Protocol (ARP) requests and responses from a host configured with a static IP address when dynamic ARP inspection is enabled. Use the **no** form of this command to return to the default settings.

**ip arp inspection filter** *arp-acl-name* **vlan** *vlan-range* [**static**]

**no ip arp inspection filter** *arp-acl-name* **vlan** *vlan-range* [**static**]

### Syntax Description

<i>arp-acl-name</i>	ARP access control list (ACL) name.
<i>vlan-range</i>	VLAN number or range.  You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
<b>static</b>	(Optional) Specify <b>static</b> to treat implicit denies in the ARP ACL as explicit denies and to drop packets that do not match any previous clauses in the ACL. DHCP bindings are not used.  If you do not specify this keyword, it means that there is no explicit deny in the ACL that denies the packet, and DHCP bindings determine whether a packet is permitted or denied if the packet does not match any clauses in the ACL.

### Defaults

No defined ARP ACLs are applied to any VLAN.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

When an ARP ACL is applied to a VLAN for dynamic ARP inspection, only the ARP packets with IP-to-MAC address bindings are compared against the ACL. If the ACL permits a packet, the switch forwards it. All other packet types are bridged in the ingress VLAN without validation.

If the switch denies a packet because of an explicit deny statement in the ACL, the packet is dropped. If the switch denies a packet because of an implicit deny statement, the packet is then compared against the list of DHCP bindings (unless the ACL is *static*, which means that packets are not compared against the bindings).

Use the **arp access-list** *acl-name* global configuration command to define the ARP ACL or to add clauses to the end of a predefined list.

**Examples**

This example shows how to apply the ARP ACL *static-hosts* to VLAN 1 for dynamic ARP inspection:

```
Switch(config)# ip arp inspection filter static-hosts vlan 1
```

You can verify your settings by entering the **show ip arp inspection vlan 1** privileged EXEC command.

**Related Commands**

Command	Description
<a href="#">arp access-list</a>	Defines an ARP ACL.
<a href="#">deny (ARP access-list configuration)</a>	Denies an ARP packet based on matches against the DHCP bindings.
<a href="#">permit (ARP access-list configuration)</a>	Permits an ARP packet based on matches against the DHCP bindings.
<a href="#">show arp access-list</a>	Displays detailed information about ARP access lists.
<a href="#">show ip arp inspection vlan <i>vlan-range</i></a>	Displays the configuration and the operating state of dynamic ARP inspection for the specified VLAN.



## ip arp inspection limit

Use the **ip arp inspection limit** interface configuration command to limit the rate of incoming Address Resolution Protocol (ARP) requests and responses on an interface. It prevents dynamic ARP inspection from using all of the switch resources if a denial-of-service attack occurs. Use the **no** form of this command to return to the default settings.

```
ip arp inspection limit {rate pps [burst interval seconds] | none}
```

```
no ip arp inspection limit
```

### Syntax Description

<b>rate</b> <i>pps</i>	Specify an upper limit for the number of incoming packets processed per second. The range is 0 to 2048 packets per second (pps).
<b>burst interval</b> <i>seconds</i>	(Optional) Specify the consecutive interval in seconds, over which the interface is monitored for a high rate of ARP packets. The range is 1 to 15 seconds.
<b>none</b>	Specify no upper limit for the rate of incoming ARP packets that can be processed.

### Defaults

The rate is 15 pps on untrusted interfaces, assuming that the network is a switched network with a host connecting to as many as 15 new hosts per second.

The rate is unlimited on all trusted interfaces.

The burst interval is 1 second.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

The rate applies to both trusted and untrusted interfaces. Configure appropriate rates on trunks to process packets across multiple dynamic ARP inspection-enabled VLANs, or use the **none** keyword to make the rate unlimited.

After a switch receives more than the configured rate of packets every second consecutively over a number of burst seconds, the interface is placed into an error-disabled state.

Unless you explicitly configure a rate limit on an interface, changing the trust state of the interface also changes its rate limit to the default value for that trust state. After you configure the rate limit, the interface retains the rate limit even when its trust state is changed. If you enter the **no ip arp inspection limit** interface configuration command, the interface reverts to its default rate limit.

You should configure trunk ports with higher rates to reflect their aggregation. When the rate of incoming packets exceeds the user-configured rate, the switch places the interface into an error-disabled state. The error-disable recovery feature automatically removes the port from the error-disabled state according to the recovery setting.

## ip arp inspection limit

The rate of incoming ARP packets on EtherChannel ports equals the sum of the incoming rate of ARP packets from all the channel members. Configure the rate limit for EtherChannel ports only after examining the rate of incoming ARP packets on all the channel members.

### Examples

This example shows how to limit the rate of incoming ARP requests on a port to 25 pps and to set the interface monitoring interval to 5 consecutive seconds:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip arp inspection limit rate 25 burst interval 5
```

You can verify your settings by entering the **show ip arp inspection interfaces** *interface-id* privileged EXEC command.

### Related Commands

Command	Description
<a href="#">show ip arp inspection interfaces</a>	Displays the trust state and the rate limit of ARP packets for the specified interface or all interfaces.

## ip arp inspection log-buffer

Use the **ip arp inspection log-buffer** global configuration command to configure the dynamic Address Resolution Protocol (ARP) inspection logging buffer. Use the **no** form of this command to return to the default settings.

```
ip arp inspection log-buffer {entries number | logs number interval seconds}
```

```
no ip arp inspection log-buffer {entries | logs}
```

### Syntax Description

<b>entries</b> <i>number</i>	Number of entries to be logged in the buffer. The range is 0 to 1024.
<b>logs</b> <i>number</i>	Number of entries needed in the specified interval to generate system messages.
<b>interval</b> <i>seconds</i>	For <b>logs</b> <i>number</i> , the range is 0 to 1024. A 0 value means that the entry is placed in the log buffer, but a system message is not generated.  For <b>interval</b> <i>seconds</i> , the range is 0 to 86400 seconds (1 day). A 0 value means that a system message is immediately generated (and the log buffer is always empty).

### Defaults

When dynamic ARP inspection is enabled, denied or dropped ARP packets are logged.

The number of log entries is 32.

The number of system messages is limited to 5 per second.

The logging-rate interval is 1 second.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

A value of 0 is not allowed for both the **logs** and the **interval** keywords.

The **logs** and **interval** settings interact. If the **logs** *number* X is greater than **interval** *seconds* Y, X divided by Y (X/Y) system messages are sent every second. Otherwise, one system message is sent every Y divided by X (Y/X) seconds. For example, if the **logs** *number* is 20 and the **interval** *seconds* is 4, the switch generates system messages for five entries every second while there are entries in the log buffer.

A log buffer entry can represent more than one packet. For example, if an interface receives many packets on the same VLAN with the same ARP parameters, the switch combines the packets as one entry in the log buffer and generates a system message as a single entry.

If the log buffer overflows, it means that a log event does not fit into the log buffer, and the output display for the **show ip arp inspection log** privileged EXEC command is affected. A -- in the output display appears in place of all data except the packet count and the time. No other statistics are provided for the entry. If you see this entry in the display, increase the number of entries in the log buffer, or increase the logging rate.

**Examples**

This example shows how to configure the logging buffer to hold up to 45 entries:

```
Switch(config)# ip arp inspection log-buffer entries 45
```

This example shows how to configure the logging rate to 20 log entries per 4 seconds. With this configuration, the switch generates system messages for five entries every second while there are entries in the log buffer.

```
Switch(config)# ip arp inspection log-buffer logs 20 interval 4
```

You can verify your settings by entering the **show ip arp inspection log** privileged EXEC command.

**Related Commands**

Command	Description
<a href="#">arp access-list</a>	Defines an ARP access control list (ACL).
<a href="#">clear ip arp inspection log</a>	Clears the dynamic ARP inspection log buffer.
<a href="#">ip arp inspection vlan logging</a>	Controls the type of packets that are logged per VLAN.
<a href="#">show ip arp inspection log</a>	Displays the configuration and contents of the dynamic ARP inspection log buffer.

# ip arp inspection trust

Use the **ip arp inspection trust** interface configuration command to configure an interface trust state that determines which incoming Address Resolution Protocol (ARP) packets are inspected. Use the **no** form of this command to return to the default setting.

**ip arp inspection trust**

**no ip arp inspection trust**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The interface is untrusted.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The switch does not check ARP packets that it receives on the trusted interface; it simply forwards the packets.

For untrusted interfaces, the switch intercepts all ARP requests and responses. It verifies that the intercepted packets have valid IP-to-MAC address bindings before updating the local cache and before forwarding the packet to the appropriate destination. The switch drops invalid packets and logs them in the log buffer according to the logging configuration specified with the **ip arp inspection vlan logging** global configuration command.

## Examples

This example shows how to configure a port to be trusted:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip arp inspection trust
```

You can verify your setting by entering the **show ip arp inspection interfaces** *interface-id* privileged EXEC command.

## Related Commands

Command	Description
<b>ip arp inspection log-buffer</b>	Configures the dynamic ARP inspection logging buffer.
<b>show ip arp inspection interfaces</b>	Displays the trust state and the rate limit of ARP packets for the specified interface or all interfaces.
<b>show ip arp inspection log</b>	Displays the configuration and contents of the dynamic ARP inspection log buffer.

## ip arp inspection validate

Use the **ip arp inspection validate** global configuration command to perform specific checks for dynamic Address Resolution Protocol (ARP) inspection. Use the **no** form of this command to return to the default settings.

```
ip arp inspection validate {[src-mac] [dst-mac] [ip [allow zeros]]}
```

```
no ip arp inspection validate [src-mac] [dst-mac] [ip [allow zeros]]
```

### Syntax Description

<b>src-mac</b>	Compare the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses.  When enabled, packets with different MAC addresses are classified as invalid and are dropped.
<b>dst-mac</b>	Compare the destination MAC address in the Ethernet header against the target MAC address in ARP body. This check is performed for ARP responses.  When enabled, packets with different MAC addresses are classified as invalid and are dropped.
<b>ip</b>	Compare the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses.  Sender IP addresses are compared in all ARP requests and responses. Target IP addresses are checked only in ARP responses.
<b>allow-zeros</b>	Modifies the IP validation test so that ARPs with a sender address of 0.0.0.0 (ARP probes) are not denied.

### Defaults

No checks are performed.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

You must specify at least one of the keywords. Each command overrides the configuration of the previous command; that is, if a command enables **src-mac** and **dst-mac** validations, and a second command enables IP validation only, the **src-mac** and **dst-mac** validations are disabled as a result of the second command.

The **allow-zeros** keyword interacts with ARP access control lists (ACLs) in this way:

- If you configure an ARP ACL to deny ARP probes, they are dropped even if the **allow-zero** keyword is specified.

- If you configure an ARP ACL that specifically permits ARP probes and configure the **ip arp inspection validate ip** command, ARP probes are dropped unless you enter the **allow-zeros** keyword.

The **no** form of the command disables only the specified checks. If none of the options are enabled, all checks are disabled.

---

**Examples**

This example show how to enable source MAC validation:

```
Switch(config)# ip arp inspection validate src-mac
```

You can verify your setting by entering the **show ip arp inspection vlan** *vlan-range* privileged EXEC command.

---

**Related Commands**

Command	Description
<a href="#">show ip arp inspection</a> <b>vlan</b> <i>vlan-range</i>	Displays the configuration and the operating state of dynamic ARP inspection for the specified VLAN.

# ip arp inspection vlan

Use the **ip arp inspection vlan** global configuration command to enable dynamic Address Resolution Protocol (ARP) inspection on a per-VLAN basis. Use the **no** form of this command to return to the default setting.

**ip arp inspection vlan** *vlan-range*

**no ip arp inspection vlan** *vlan-range*

## Syntax Description

<i>vlan-range</i>	VLAN number or range. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
-------------------	---

## Defaults

ARP inspection is disabled on all VLANs.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

You must specify the VLANs on which to enable dynamic ARP inspection.

Dynamic ARP inspection is supported on access ports, trunk ports, EtherChannel ports, or private VLAN ports.

## Examples

This example shows how to enable dynamic ARP inspection on VLAN 1:

```
Switch(config)# ip arp inspection vlan 1
```

You can verify your setting by entering the **show ip arp inspection vlan** *vlan-range* privileged EXEC command.

## Related Commands

Command	Description
<a href="#">arp access-list</a>	Defines an ARP access control list (ACL).
<a href="#">show ip arp inspection vlan</a> <i>vlan-range</i>	Displays the configuration and the operating state of dynamic ARP inspection for the specified VLAN.



# ip arp inspection vlan logging

Use the **ip arp inspection vlan logging** global configuration command to control the type of packets that are logged per VLAN. Use the **no** form of this command to disable this logging control.

```
ip arp inspection vlan vlan-range logging {acl-match {matchlog | none} | dhcp-bindings {all | none | permit} | arp-probe}
```

```
no ip arp inspection vlan vlan-range logging {acl-match | dhcp-bindings | arp-probe}
```

## Syntax Description

<i>vlan-range</i>	Specify the VLANs configured for logging.  You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
<b>acl-match</b> { <b>matchlog</b>   <b>none</b> }	Specify that the logging of packets is based on access control list (ACL) matches.  The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>matchlog</b>—Log packets based on the logging configuration specified in the access control entries (ACE). If you specify the <b>matchlog</b> keyword in this command and the <b>log</b> keyword in the <b>permit</b> or <b>deny</b> ARP access-list configuration command, Address Resolution Protocol (ARP) packets permitted or denied by the ACL are logged.</li> <li>• <b>none</b>—Do not log packets that match ACLs.</li> </ul>
<b>dhcp-bindings</b> { <b>permit</b>   <b>all</b>   <b>none</b> }	Specify the logging of packets is based on Dynamic Host Configuration Protocol (DHCP) binding matches.  The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>all</b>—Log all packets that match DHCP bindings.</li> <li>• <b>none</b>—Do not log packets that match DHCP bindings.</li> <li>• <b>permit</b>—Log DHCP-binding permitted packets.</li> </ul>
<b>arp-probe</b>	Specify logging of packets permitted specifically because they are ARP probes.

## Defaults

All denied or all dropped packets are logged. ARP probe packets are not logged.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

**Usage Guidelines**

The term *logged* means that the entry is placed into the log buffer and that a system message is generated. The **acl-match** and **dhcp-bindings** keywords merge with each other; that is, when you configure an ACL match, the DHCP bindings configuration is not disabled. Use the **no** form of the command to reset the logging criteria to their defaults. If neither option is specified, all types of logging are reset to log when ARP packets are denied. These are the options:

- **acl-match**—Logging on ACL matches is reset to log on deny.
- **dhcp-bindings**—Logging on DHCP binding matches is reset to log on deny.

If neither the **acl-match** or the **dhcp-bindings** keywords are specified, all denied packets are logged.

The implicit deny at the end of an ACL does not include the **log** keyword. This means that when you use the **static** keyword in the **ip arp inspection filter vlan** global configuration command, the ACL overrides the DHCP bindings. Some denied packets might not be logged unless you explicitly specify the **deny ip any mac any log** ACE at the end of the ARP ACL.

**Examples**

This example shows how to configure ARP inspection on VLAN 1 to log packets that match the **permit** commands in the ACL:

```
Switch(config)# arp access-list test1
Switch(config-arp-nacl)# permit request ip any mac any log
Switch(config-arp-nacl)# permit response ip any any mac any any log
Switch(config-arp-nacl)# exit
Switch(config)# ip arp inspection vlan 1 logging acl-match matchlog
```

You can verify your settings by entering the **show ip arp inspection vlan *vlan-range*** privileged EXEC command.

**Related Commands**

Command	Description
<b>arp access-list</b>	Defines an ARP ACL.
<b>clear ip arp inspection log</b>	Clears the dynamic ARP inspection log buffer.
<b>ip arp inspection log-buffer</b>	Configures the dynamic ARP inspection logging buffer.
<b>show ip arp inspection log</b>	Displays the configuration and contents of the dynamic ARP inspection log buffer.
<b>show ip arp inspection vlan <i>vlan-range</i></b>	Displays the configuration and the operating state of dynamic ARP inspection for the specified VLAN.

# ip device tracking maximum

Use the **ip device tracking maximum** command to enable IP port security binding tracking on a Layer 2 port. Use the **no** form of this command to disable IP port security on untrusted Layer 2 interfaces.

**ip device tracking maximum** {*number*}

**no ip device tracking maximum** {*number*}

## Syntax Description

<i>number</i>	Specify the number of bindings created in the IP device tracking table for a port. valid values are from 0 to 2048.
---------------	---

## Defaults

This command has no default setting.

## Command Modes

Interface configuration mode

## Command History

Release	Modification
12.2(52)SE	This command was introduced.

## Examples

This example shows how to enable IP port security with IP-MAC filters on a Layer 2 access port:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet 0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# end
```

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

## Related Commands

Command	Description
<a href="#">ip verify source</a>	Enables IP source guard on untrusted Layer 2 interfaces.
<a href="#">show ip verify source</a>	Displays the IP source guard configuration and filters on a particular interface.

# ip dhcp snooping

Use the **ip dhcp snooping** global configuration command to globally enable DHCP snooping. Use the **no** form of this command to return to the default setting.

**ip dhcp snooping**

**no ip dhcp snooping**

**Syntax Description** This command has no arguments or keywords.

**Defaults** DHCP snooping is disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** For any DHCP snooping configuration to take effect, you must globally enable DHCP snooping. DHCP snooping is not active until you enable snooping on a VLAN by using the **ip dhcp snooping vlan *vlan-id*** global configuration command.

**Examples** This example shows how to enable DHCP snooping:

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

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

Related Commands	Command	Description
	<a href="#">ip dhcp snooping vlan</a>	Enables DHCP snooping on a VLAN.
	<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.
	<a href="#">show ip dhcp snooping binding</a>	Displays the DHCP snooping binding information.

# ip dhcp snooping binding

Use the **ip dhcp snooping binding** privileged EXEC command to configure the DHCP snooping binding database and to add binding entries to the database. Use the **no** form of this command to delete entries from the binding database.

**ip dhcp snooping binding** *mac-address* **vlan** *vlan-id* *ip-address* **interface** *interface-id* **expiry** *seconds*

**no ip dhcp snooping binding** *mac-address* **vlan** *vlan-id* *ip-address* **interface** *interface-id*

Syntax Description		
<i>mac-address</i>		Specify a MAC address.
<b>vlan</b> <i>vlan-id</i>		Specify a VLAN number. The range is from 1 to 4904.
<i>ip-address</i>		Specify an IP address.
<b>interface</b> <i>interface-id</i>		Specify an interface on which to add or delete a binding entry.
<b>expiry</b> <i>seconds</i>		Specify the interval (in seconds) after which the binding entry is no longer valid. The range is from 1 to 4294967295.

**Defaults** No default database is defined.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** Use this command when you are testing or debugging the switch.

In the DHCP snooping binding database, each database entry, also referred to a binding, has an IP address, an associated MAC address, the lease time (in hexadecimal format), the interface to which the binding applies, and the VLAN to which the interface belongs. The database can have up to 8192 bindings.

Use the **show ip dhcp snooping binding** privileged EXEC command to display only the dynamically configured bindings. Use the **show ip source binding** privileged EXEC command to display the dynamically and statically configured bindings.

**Examples** This example shows how to generate a DHCP binding configuration with an expiration time of 1000 seconds on a port in VLAN 1:

```
Switch# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface
gigabitethernet0/1 expiry 1000
```

You can verify your settings by entering the **show ip dhcp snooping binding** or the **show ip dhcp source binding** privileged EXEC command.

## ■ ip dhcp snooping binding

Related Commands	Command	Description
	<a href="#">ip dhcp snooping</a>	Enables DHCP snooping on a VLAN.
	<a href="#">show ip dhcp snooping binding</a>	Displays the dynamically configured bindings in the DHCP snooping binding database and the configuration information.
	<a href="#">show ip source binding</a>	Displays the dynamically and statically configured bindings in the DHCP snooping binding database.

## ip dhcp snooping database

Use the **ip dhcp snooping database** global configuration command to configure the DHCP snooping binding database agent. Use the **no** form of this command to disable the agent, to reset the timeout value, or to reset the write-delay value.

```
ip dhcp snooping database {{flash:/filename | ftp://user:password@host/filename |  
http://[[username:password]@]{hostname \ host-ip}/[directory]/image-name.tar |  
rcp://user@host/filename | tftp://host/filename} | timeout seconds | write-delay seconds}
```

```
no ip dhcp snooping database [timeout | write-delay]
```

Syntax Description		
<b>flash:</b> / <i>filename</i>		Specify that the database agent or the binding file is in the flash memory.
<b>ftp:</b> // <i>user:password@host/filename</i>		Specify that the database agent or the binding file is on an FTP server.
<b>http:</b> //[[ <i>username:password</i> ]@]{ <i>hostname</i> \ <i>host-ip</i> }/[ <i>directory</i> ]/ <i>image-name.tar</i>		Specify that the database agent or the binding file is on an FTP server.
<b>rcp:</b> // <i>user@host/filename</i>		Specify that the database agent or the binding file is on a Remote Control Protocol (RCP) server.
<b>tftp:</b> // <i>host/filename</i>		Specify that the database agent or the binding file is on a TFTP server.
<b>timeout</b> <i>seconds</i>		Specify (in seconds) when to stop the database transfer process after the DHCP snooping binding database changes.  The default is 300 seconds. The range is from 0 to 86400. Use 0 to define an infinite duration.
<b>write-delay</b> <i>seconds</i>		Specify (in seconds) the duration for which the transfer should be delayed after the binding database changes. The default is 300 seconds. The range is from 15 to 86400.

### Defaults

The URL for the database agent or binding file is not defined.

The timeout value is 300 seconds (5 minutes).

The write-delay value is 300 seconds (5 minutes).

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

**Usage Guidelines**

The DHCP snooping binding database can have up to 8192 bindings.

To ensure that the lease time in the database is accurate, we recommend that Network Time Protocol (NTP) is enabled and configured for these features:

- NTP authentication
- NTP peer and server associations
- NTP broadcast service
- NTP access restrictions
- NTP packet source IP address

If NTP is configured, the switch writes binding changes to the binding file only when the switch system clock is synchronized with NTP.

Because both NVRAM and the flash memory have limited storage capacity, we recommend that you store a binding file on a TFTP server. You must create an empty file at the configured URL on network-based URLs (such as TFTP and FTP) before the switch can write bindings to the binding file at that URL for the first time.

Use the **no ip dhcp snooping database** command to disable the agent.

Use the **no ip dhcp snooping database timeout** command to reset the timeout value.

Use the **no ip dhcp snooping database write-delay** command to reset the write-delay value.

**Examples**

This example shows how to store a binding file at an IP address of 10.1.1.1 that is in a directory called *directory*. A file named *file* must be present on the TFTP server.

```
Switch(config)# ip dhcp snooping database tftp://10.1.1.1/directory/file
```

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

**Related Commands**

Command	Description
<a href="#">ip dhcp snooping</a>	Enables DHCP snooping on a VLAN.
<a href="#">ip dhcp snooping binding</a>	Configures the DHCP snooping binding database.
<a href="#">show ip dhcp snooping database</a>	Displays the status of DHCP snooping database agent.



# ip dhcp snooping information option

Use the **ip dhcp snooping information option** global configuration command to enable DHCP option-82 data insertion. Use the **no** form of this command to disable DHCP option-82 data insertion.

**ip dhcp snooping information option**

**no ip dhcp snooping information option**

**Syntax Description** This command has no arguments or keywords.

**Defaults** DHCP option-82 data insertion is enabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** You must globally enable DHCP snooping by using the **ip dhcp snooping** global configuration command for any DHCP snooping configuration to take effect.

When the option-82 feature is enabled and a switch receives a DHCP request from a host, it adds the option-82 information in the packet. The option-82 information contains the switch MAC address (the remote ID suboption) and the port identifier, **vlan-mod-port**, from which the packet is received (circuit ID suboption). The switch forwards the DHCP request that includes the option-82 field to the DHCP server.

When the DHCP server receives the packet, it can use the remote ID, the circuit ID, or both to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single remote ID or a circuit ID. Then the DHCP server echoes the option-82 field in the DHCP reply.

The DHCP server unicasts the reply to the switch if the request was relayed to the server by the switch. When the client and server are on the same subnet, the server broadcasts the reply. The switch inspects the remote ID and possibly the circuit ID fields to verify that it originally inserted the option-82 data. The switch removes the option-82 field and forwards the packet to the switch port that connects to the DHCP host that sent the DHCP request.

**Examples** This example shows how to enable DHCP option-82 data insertion:

```
Switch(config)# ip dhcp snooping information option
```

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

## ■ ip dhcp snooping information option

Related Commands	Command	Description
	<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.
	<a href="#">show ip dhcp snooping binding</a>	Displays the DHCP snooping binding information.

# ip dhcp snooping information option allowed-untrusted

Use the **ip dhcp snooping information option allowed-untrusted** global configuration command on an aggregation switch to configure it to accept DHCP packets with option-82 information that are received on untrusted ports that might be connected to an edge switch. Use the **no** form of this command to configure the switch to drop these packets from the edge switch.

**ip dhcp snooping information option allowed-untrusted**

**no ip dhcp snooping information option allowed-untrusted**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The switch drops DHCP packets with option-82 information that are received on untrusted ports that might be connected to an edge switch.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

You might want an edge switch to which a host is connected to insert DHCP option-82 information at the edge of your network. You might also want to enable DHCP security features, such as DHCP snooping, IP source guard, or dynamic Address Resolution Protocol (ARP) inspection, on an aggregation switch. However, if DHCP snooping is enabled on the aggregation switch, the switch drops packets with option-82 information that are received on an untrusted port and does not learn DHCP snooping bindings for connected devices on a trusted interface.

If the edge switch to which a host is connected inserts option-82 information and you want to use DHCP snooping on an aggregation switch, enter the **ip dhcp snooping information option allowed-untrusted** command on the aggregation switch. The aggregation switch can learn the bindings for a host even though the aggregation switch receives DHCP snooping packets on an untrusted port. You can also enable DHCP security features on the aggregation switch. The port on the edge switch to which the aggregation switch is connected must be configured as a trusted port.



### Note

Do not enter the **ip dhcp snooping information option allowed-untrusted** command on an aggregation switch to which an untrusted device is connected. If you enter this command, an untrusted device might spoof the option-82 information.

## Examples

This example shows how to configure an access switch to not check the option-82 information in untrusted packets from an edge switch and to accept the packets:

```
Switch(config)# ip dhcp snooping information option allowed-untrusted
```

## ■ ip dhcp snooping information option allowed-untrusted

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

Related Commands	Command	Description
	<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.
	<a href="#">show ip dhcp snooping binding</a>	Displays the DHCP snooping binding information.

# ip dhcp snooping information option format remote-id

Use the **ip dhcp snooping information option format remote-id** global configuration command to configure the option-82 remote-ID suboption. Use the **no** form of this command to configure the default remote-ID suboption.

**ip dhcp snooping information option format remote-id** [*string ASCII-string* | *hostname*]

**no ip dhcp snooping information option format remote-id**

## Syntax Description

<b>string</b> <i>ASCII-string</i>	Specify a remote ID, using from 1 to 63 ASCII characters (no spaces).
<b>hostname</b>	Specify the switch hostname as the remote ID.

## Defaults

The switch MAC address is the remote ID.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

You must globally enable DHCP snooping by using the **ip dhcp snooping** global configuration command for any DHCP snooping configuration to take effect.

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.



### Note

If the hostname exceeds 63 characters, it is truncated to 63 characters in the remote-ID configuration.

## Examples

This example shows how to configure the option-82 remote-ID suboption:

```
Switch(config)# ip dhcp snooping information option format remote-id hostname
```

You can verify your settings by entering the **show ip dhcp snooping** user EXEC command.

## Related Commands

Command	Description
<a href="#">ip dhcp snooping vlan information option format-type circuit-id string</a>	Configures the option-82 circuit-ID suboption.
<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.

## ip dhcp snooping limit rate

Use the **ip dhcp snooping limit rate** interface configuration command to configure the number of DHCP messages an interface can receive per second. Use the **no** form of this command to return to the default setting.

**ip dhcp snooping limit rate** *rate*

**no ip dhcp snooping limit rate**

<b>Syntax Description</b>	<i>rate</i>	Number of DHCP messages an interface can receive per second. The range is 1 to 2048.
---------------------------	-------------	--

**Defaults** DHCP snooping rate limiting is disabled.

**Command Modes** Interface configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

**Usage Guidelines** Normally, the rate limit applies to untrusted interfaces. If you want to configure rate limiting for trusted interfaces, keep in mind that trusted interfaces might aggregate DHCP traffic on multiple VLANs (some of which might not be snooped) in the switch, and you will need to adjust the interface rate limits to a higher value.

If the rate limit is exceeded, the interface is error-disabled. If you enabled error recovery by entering the **errdisable recovery dhcp-rate-limit** global configuration command, the interface retries the operation again when all the causes have timed out. If the error-recovery mechanism is not enabled, the interface stays in the error-disabled state until you enter the **shutdown** and **no shutdown** interface configuration commands.

**Examples** This example shows how to set a message rate limit of 150 messages per second on an interface:

```
Switch(config-if)# ip dhcp snooping limit rate 150
```

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">errdisable recovery</a>	Configures the recover mechanism.
	<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.
	<a href="#">show ip dhcp snooping binding</a>	Displays the DHCP snooping binding information.

# ip dhcp snooping trust

Use the **ip dhcp snooping trust** interface configuration command to configure a port as trusted for DHCP snooping purposes. Use the **no** form of this command to return to the default setting.

**ip dhcp snooping trust**

**no ip dhcp snooping trust**

**Syntax Description** This command has no arguments or keywords.

**Defaults** DHCP snooping trust is disabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** Configure as trusted ports those that are connected to a DHCP server or to other switches or routers. Configure as untrusted ports those that are connected to DHCP clients.

**Examples** This example shows how to enable DHCP snooping trust on a port:

```
Switch(config-if)# ip dhcp snooping trust
```

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

Related Commands	Command	Description
	<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.
	<a href="#">show ip dhcp snooping binding</a>	Displays the DHCP snooping binding information.

## ip dhcp snooping verify mac-address

Use the **ip dhcp snooping verify mac-address** global configuration command to configure the switch to verify on an untrusted port that the source MAC address in a DHCP packet matches the client hardware address. Use the **no** form of this command to configure the switch to not verify the MAC addresses.

**ip dhcp snooping verify mac-address**

**no ip dhcp snooping verify mac-address**

**Syntax Description** This command has no arguments or keywords.

**Defaults** The switch verifies the source MAC address in a DHCP packet that is received on untrusted ports matches the client hardware address in the packet.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** In a service-provider network, when a switch receives a packet from a DHCP client on an untrusted port, it automatically verifies that the source MAC address and the DHCP client hardware address match. If the addresses match, the switch forwards the packet. If the addresses do not match, the switch drops the packet.

**Examples** This example shows how to disable the MAC address verification:

```
Switch(config)# no ip dhcp snooping verify mac-address
```

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

Related Commands	Command	Description
	<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.



# ip dhcp snooping vlan

Use the **ip dhcp snooping vlan** global configuration command to enable DHCP snooping on a VLAN. Use the **no** form of this command to disable DHCP snooping on a VLAN.

**ip dhcp snooping vlan** *vlan-range*

**no ip dhcp snooping vlan** *vlan-range*

## Syntax Description

<b>vlan</b> <i>vlan-range</i>	Specify a VLAN ID or a range of VLANs on which to enable DHCP snooping. The range is 1 to 4094.  You can enter a single VLAN ID identified by VLAN ID number, a series of VLAN IDs separated by commas, a range of VLAN IDs separated by hyphens, or a range of VLAN IDs separated by entering the starting and ending VLAN IDs separated by a space.
-------------------------------	---

## Defaults

DHCP snooping is disabled on all VLANs.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

You must first globally enable DHCP snooping before enabling DHCP snooping on a VLAN.

## Examples

This example shows how to enable DHCP snooping on VLAN 10:

```
Switch(config)# ip dhcp snooping vlan 10
```

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

## Related Commands

Command	Description
<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.
<a href="#">show ip dhcp snooping binding</a>	Displays the DHCP snooping binding information.

# ip dhcp snooping vlan information option format-type circuit-id string

Use the **ip dhcp snooping vlan information option format-type circuit-id string** interface configuration command to configure the option-82 circuit-ID suboption. Use the **no** form of this command to configure the default circuit-ID suboption.

**ip dhcp snooping vlan** *vlan* **information option format-type circuit-id** [**override**] **string** *ASCII-string*

**no ip dhcp snooping vlan** *vlan* **information option format-type circuit-id** [**override**] **string**

Syntax Description		
<b>vlan</b> <i>vlan</i>		Specify the VLAN ID. The range is 1 to 4094.
<b>override</b>		(Optional) Specify an override string, using from 3 to 63 ASCII characters (no spaces).
<b>string</b> <i>ASCII-string</i>		Specify a circuit ID, using from 3 to 63 ASCII characters (no spaces).

**Defaults** The switch VLAN and the port identifier, in the format **vlan-mod-port**, is the default circuit ID.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.
	12.2(52)SE	The <b>override</b> keyword was added.

**Usage Guidelines** You must globally enable DHCP snooping by using the **ip dhcp snooping** global configuration command for any DHCP snooping configuration to take effect.

When the option-82 feature is enabled, the default circuit-ID suboption is the switch VLAN and the port identifier, in the format **vlan-mod-port**. This command allows you to configure a string of ASCII characters to be the circuit ID. When you want to override the **vlan-mod-port** format type and instead use the circuit-ID to define subscriber information, use the **override** keyword.



**Note**

When configuring a large number of circuit IDs on a switch, consider the impact of lengthy character strings on the NVRAM or flash memory. If the circuit-ID configurations, combined with other data, exceed the capacity of the NVRAM or the flash memory, an error message appears.

**Examples** This example shows how to configure the option-82 circuit-ID suboption:

```
Switch(config-if)# ip dhcp snooping vlan 250 information option format-type circuit-id
string customerABC-250-0-0
```

This example shows how to configure the option-82 circuit-ID override suboption:

```
Switch(config-if)# ip dhcp snooping vlan 250 information option format-type circuit-id  
override string testcustomer
```

You can verify your settings by entering the **show ip dhcp snooping** user EXEC command.

**Note**

The **show ip dhcp snooping user EXEC** command only displays the global command output, including a remote-ID configuration. It does not display any per-interface, per-VLAN string that you have configured for the circuit ID.

**Related Commands**

Command	Description
<a href="#">ip dhcp snooping information option format remote-id</a>	Configures the option-82 remote-ID suboption.
<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.

## ip igmp filter

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

**ip igmp filter** *profile number*

**no ip igmp filter**

<b>Syntax Description</b>	<i>profile number</i> The IGMP profile number to be applied. The range is 1 to 4294967295.
---------------------------	--

<b>Defaults</b>	No IGMP filters are applied.
-----------------	------------------------------

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

<b>Usage Guidelines</b>	<p>You can apply IGMP filters only to Layer 2 physical interfaces.</p> <p>You cannot apply IGMP filters to routed ports, switch virtual interfaces (SVIs), or ports that belong to an EtherChannel group.</p> <p>An IGMP profile can be applied to one or more switch port interfaces, but one port can have only one profile applied to it.</p>
-------------------------	--

<b>Examples</b>	This example shows how to apply IGMP profile 22 to a port.
-----------------	--

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

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

Related Commands	Command	Description
	<a href="#">ip igmp profile</a>	Configures the specified IGMP profile number.
	<a href="#">show ip dhcp snooping statistics</a>	Displays the characteristics of the specified IGMP profile.
	<a href="#">show running-config interface interface-id</a>	Displays the running configuration on the switch interface, including the IGMP profile (if any) that is applied to an interface. For syntax information, select <b>Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 &gt; File Management Commands &gt; Configuration File Management Commands</b> .

## ip igmp max-groups

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

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

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

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

### Defaults

The default maximum number of groups is no limit.

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

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

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

Follow these guidelines when configuring the IGMP throttling action:

- If you configure the throttling action as **deny** and set the maximum group limitation, the entries that were previously in the forwarding table are not removed but are aged out. After these entries are aged out, when the maximum number of entries is in the forwarding table, the switch drops the next IGMP report received on the interface.

- If you configure the throttling action as **replace** and set the maximum group limitation, the entries that were previously in the forwarding table are removed. When the maximum number of entries is in the forwarding table, the switch replaces a randomly-selected multicast entry with the received IGMP report.
- When the maximum group limitation is set to the default (no maximum), entering the **ip igmp max-groups {deny | replace}** command has no effect.

### Examples

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

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

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

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

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

### Related Commands

Command	Description
<b>show running-config interface</b> <i>interface-id</i>	Displays the running configuration on the switch interface, including the maximum number of IGMP groups that an interface can join and the throttling action. For syntax information, select <b>Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 &gt; File Management Commands &gt; Configuration File Management Commands</b> .

# ip igmp profile

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

**ip igmp profile** *profile number*

**no ip igmp profile** *profile number*

<b>Syntax Description</b>	<i>profile number</i> The IGMP profile number being configured. The range is 1 to 4294967295.
---------------------------	---

<b>Defaults</b>	No IGMP profiles are defined. When configured, the default action for matching an IGMP profile is to deny matching addresses.
-----------------	---

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

<b>Usage Guidelines</b>	When you are in IGMP profile configuration mode, you can create the profile by using these commands:
-------------------------	--

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

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

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

<b>Examples</b>	This example shows how to configure IGMP profile 40 that permits the specified range of IP multicast addresses.
-----------------	---

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

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



Related Commands	Command	Description
	<a href="#">ip igmp filter</a>	Applies the IGMP profile to the specified interface.
	<a href="#">show ip dhcp snooping statistics</a>	Displays the characteristics of all IGMP profiles or the specified IGMP profile number.

## ip igmp snooping

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

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

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

<b>Syntax Description</b>	<b>vlan</b> <i>vlan-id</i>	(Optional) Enable IGMP snooping on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
---------------------------	----------------------------	---

<b>Defaults</b>	IGMP snooping is globally enabled on the switch. IGMP snooping is enabled on VLAN interfaces.
-----------------	--

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

<b>Usage Guidelines</b>	When IGMP snooping is enabled globally, it is enabled in all the existing VLAN interfaces. When IGMP snooping is disabled globally, it is disabled on all the existing VLAN interfaces.  VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.
-------------------------	--

**Examples** This example shows how to globally enable IGMP snooping:

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

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

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

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

Related Commands	Command	Description
	<a href="#">ip igmp snooping report-suppression</a>	Enables IGMP report suppression.
	<a href="#">show ip igmp snooping</a>	Displays the snooping configuration.
	<a href="#">show ip igmp snooping groups</a>	Displays IGMP snooping multicast information.
	<a href="#">show ip igmp snooping mrouter</a>	Displays the IGMP snooping router ports.
	<a href="#">show ip igmp snooping querier detail</a>	Displays the configuration and operation information for the IGMP querier configured on a switch.

# ip igmp snooping last-member-query-interval

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

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

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

## Syntax Description

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

## Defaults

The default timeout setting is 1000 milliseconds.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

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

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

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

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

The configuration is saved in NVRAM.

## Examples

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

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

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

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

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

Related Commands	Command	Description
	<a href="#">ip igmp snooping</a>	Enables IGMP snooping on the switch or on a VLAN.
	<a href="#">ip igmp snooping vlan immediate-leave</a>	Enables IGMP Immediate-Leave processing.
	<a href="#">ip igmp snooping vlan mrouter</a>	Configures a Layer 2 port as a multicast router port.
	<a href="#">ip igmp snooping vlan static</a>	Configures a Layer 2 port as a member of a group.
	<a href="#">show ip igmp snooping</a>	Displays the IGMP snooping configuration.

## ip igmp snooping querier

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

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

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

### Syntax Description

<b>vlan</b> <i>vlan-id</i>	(Optional) Enable IGMP snooping and the IGMP querier function on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
<b>address</b> <i>ip-address</i>	(Optional) Specify a source IP address. If you do not specify an IP address, the querier tries to use the global IP address configured for the IGMP querier.
<b>max-response-time</b> <i>response-time</i>	(Optional) Set the maximum time to wait for an IGMP querier report. The range is 1 to 25 seconds.
<b>query-interval</b> <i>interval-count</i>	(Optional) Set the interval between IGMP queriers. The range is 1 to 18000 seconds.
<b>tcn query</b> [ <b>count</b> <i>count</i>   <b>interval</b> <i>interval</i> ]	(Optional) Set parameters related to Topology Change Notifications (TCNs). The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>count</b> <i>count</i>—Set the number of TCN queries to be executed during the TCN interval time. The range is 1 to 10.</li> <li>• <b>interval</b> <i>interval</i>—Set the TCN query interval time. The range is 1 to 255.</li> </ul>
<b>timer expiry</b>	(Optional) Set the length of time until the IGMP querier expires. The range is 60 to 300 seconds.
<b>version</b> <i>version</i>	(Optional) Select the IGMP version number that the querier feature uses. Select 1 or 2.

### Defaults

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

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

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

**Usage Guidelines**

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

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

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

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

**Examples**

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

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

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

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

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

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

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

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

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

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

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

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

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

**Related Commands**

Command	Description
<a href="#">ip igmp snooping report-suppression</a>	Enables IGMP report suppression.
<a href="#">show ip igmp snooping</a>	Displays the IGMP snooping configuration.
<a href="#">show ip igmp snooping groups</a>	Displays IGMP snooping multicast information.
<a href="#">show ip igmp snooping mrouter</a>	Displays the IGMP snooping router ports.

## ip igmp snooping report-suppression

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

**ip igmp snooping report-suppression**

**no ip igmp snooping report-suppression**

**Syntax Description** This command has no arguments or keywords.

**Defaults** IGMP report suppression is enabled.

**Command Modes** Global configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

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

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

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

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

### Examples

This example shows how to disable report suppression:

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

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



**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">ip igmp snooping</a>	Enables IGMP snooping on the switch or on a VLAN.
<a href="#">show ip igmp snooping</a>	Displays the IGMP snooping configuration of the switch or the VLAN.

## ip igmp snooping tcn

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

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

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

### Syntax Description

**flood query count** *count* Specify the number of IGMP general queries for which the multicast traffic is flooded. The range is 1 to 10.

**query solicit** Send an IGMP leave message (global leave) to speed the process of recovering from the flood mode caused during a TCN event.

### Defaults

The TCN flood query count is 2.

The TCN query solicitation is disabled.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

You can prevent the loss of the multicast traffic that might occur because of a topology change by using this command. If you set the TCN flood query count to 1 by using the **ip igmp snooping tcn flood query count** command, the flooding stops after receiving one general query. If you set the count to 7, the flooding of multicast traffic due to the TCN event lasts until seven general queries are received. Groups are relearned based on the general queries received during the TCN event.

### Examples

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

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

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

### Related Commands

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

# ip igmp snooping tcn flood

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

**ip igmp snooping tcn flood**

**no ip igmp snooping tcn flood**

## Syntax Description

This command has no arguments or keywords.

## Defaults

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

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

When the switch receives a TCN, multicast traffic is flooded to all the ports until two general queries are received. If the switch has many ports with attached hosts that are subscribed to different multicast groups, this flooding behavior might not be desirable because the flooded traffic might exceed the capacity of the link and cause packet loss.

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

## Examples

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

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

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

## Related Commands

Command	Description
<a href="#">ip igmp snooping</a>	Enables IGMP snooping on the switch or on a VLAN.
<a href="#">ip igmp snooping tcn</a>	Configures the IGMP TCN behavior on the switch.
<a href="#">show ip igmp snooping</a>	Displays the IGMP snooping configuration of the switch or the VLAN.

# ip igmp snooping vlan immediate-leave

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

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

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

## Syntax Description

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

## Defaults

IGMP immediate-leave processing is disabled.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

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

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

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

## Examples

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

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

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

## Related Commands

Command	Description
<a href="#">ip igmp snooping report-suppression</a>	Enables IGMP report suppression.
<a href="#">show ip igmp snooping</a>	Displays the snooping configuration.
<a href="#">show ip igmp snooping groups</a>	Displays IGMP snooping multicast information.
<a href="#">show ip igmp snooping mrouter</a>	Displays the IGMP snooping router ports.
<a href="#">show ip igmp snooping querier detail</a>	Displays the configuration and operation information for the IGMP querier configured on a switch.

## ip igmp snooping vlan mrouter

Use the **ip igmp snooping vlan *vlan-id* mrouter** global configuration command to add a multicast router port or to configure the multicast learning method. Use the **no** form of this command to return to the default settings.

**ip igmp snooping vlan *vlan-id* mrouter {interface *interface-id* | learn pim-dvmrp}**

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

### Syntax Description

<i>vlan-id</i>	Enable IGMP snooping, and add the port in the specified VLAN as the multicast router port. The range is 1 to 1001 and 1006 to 4094.
<b>interface</b> <i>interface-id</i>	Specify the next-hop interface to the multicast router. Valid interfaces are physical interfaces and port channels. The port-channel range is 1 to 48.
<b>learn pim-dvmrp</b>	Specify the multicast router learning method. The only learning method supported on the Cisco ME switch is <b>pim-dvmrp</b> , which 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.

### Defaults

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
12.2(44)EY	This command was introduced.

### Usage Guidelines

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

The configuration is saved in NVRAM.

### Examples

This example shows how to configure a port as a multicast router port:

```
Switch(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet0/2
```

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

Related Commands	Command	Description
	<a href="#">ip igmp snooping report-suppression</a>	Enables IGMP report suppression.
	<a href="#">show ip igmp snooping</a>	Displays the snooping configuration.
	<a href="#">show ip igmp snooping groups</a>	Displays IGMP snooping multicast information.
	<a href="#">show ip igmp snooping mrouter</a>	Displays the IGMP snooping router ports.
	<a href="#">show ip igmp snooping querier detail</a>	Displays the configuration and operation information for the IGMP querier configured on a switch.

## ip igmp snooping vlan static

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

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

**no ip igmp snooping vlan *vlan-id* static *ip-address* interface *interface-id***

Syntax Description		
<i>vlan-id</i>	Enable IGMP snooping on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.	
<i>ip-address</i>	Add a Layer 2 port as a member of a multicast group with the specified group IP address.	
<b>interface</b> <i>interface-id</i>	Specify the interface of the member port. The keywords have these meanings:	<ul style="list-style-type: none"> <li>• <b>fastethernet</b> <i>interface number</i>—a Fast Ethernet IEEE 802.3 interface.</li> <li>• <b>gigabitethernet</b> <i>interface number</i>—a Gigabit Ethernet IEEE 802.3z interface.</li> <li>• <b>port-channel</b> <i>interface number</i>—a channel interface. The range is 0 to 48.</li> </ul>

**Defaults** By default, there are no ports statically configured as members of a multicast group.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

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

The configuration is saved in NVRAM.

**Examples** This example shows how to statically configure a port as a multicast router port:

```
Switch(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet0/2
```

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

Related Commands	Command	Description
	<a href="#">ip igmp snooping report-suppression</a>	Enables IGMP report suppression.
	<a href="#">show ip igmp snooping</a>	Displays the snooping configuration.
	<a href="#">show ip igmp snooping groups</a>	Displays IGMP snooping multicast information.
	<a href="#">show ip igmp snooping mrouter</a>	Displays the IGMP snooping router ports.
	<a href="#">show ip igmp snooping querier detail</a>	Displays the configuration and operation information for the IGMP querier configured on a switch.



# ip sla responder twamp

Use the **ip sla responder twamp** global configuration command to configure the switch as a Two-Way Active Measurement Protocol (TWAMP) responder. Use the **no** form of this command to disable the IP SLA TWAMP responder.

**ip sla responder twamp** [timeout *seconds*]

**no ip sla responder twamp** [timeout *seconds*]

Syntax	Description
<b>timeout</b> <i>seconds</i>	(Optional) Specify the number of seconds a TWAMP session can be inactive before the session ends. The range is 1-604800 seconds. The default is 900 seconds.

**Defaults** No IP SLA TWAMP responder is configured.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(52)SE	This command was introduced.

**Usage Guidelines** After entering the **ip sla responder twamp** command, you enter IP SLA TWAMP reflector configuration mode, and these configuration commands are available:

- **default**: sets a command to its defaults.
- **exit**: exits from IP SLA TWAMP reflector configuration mode.
- **no**: negates a command or resets to its defaults.
- **timeout** *seconds*: specifies the maximum time the session can be inactive before the session ends. The range is 1-604800 seconds. The default is 900 seconds.

For the TWAMP server and reflector to function, you must also configure a TWAMP control device, which serves as the client and session sender. These functions are not configured on a Cisco device.

**Examples** This example shows how to configure a switch as an IP SLA TWAMP responder:

```
Switch(config)# ip sla responder twamp
Switch(config-twamp-ref)# timeout inactivity 900
```

## ■ ip sla responder twamp

Related Commands	Command	Description
	<b>ip sla responder</b>	Enables the Cisco IOS IP Service Level Agreements (SLAs) responder for general IP SLAs operations.
	<b>ip sla server twamp</b>	Configures the switch as a Two-Way Active Measurement Protocol (TWAMP) server.
	<b>show ip sla standards</b>	(Optional) Display the IP SLAs standards configured on the switch.
	<b>show ip sla twamp connection</b> { <b>detail</b>   <b>requests</b> }	(Optional) Displays the current Cisco IOS IP Service Level Agreements (SLAs) Two-Way Active Measurement Protocol (TWAMP) connections

# ip sla server twamp

Use the **ip sla server twamp** global configuration command to configure the switch as a Two-Way Active Measurement Protocol (TWAMP) server. Use the **no** form of this command to disable the IP SLA TWAMP server.

**ip sla server twamp**

**no ip sla server twamp**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No IP SLA TWAMP server is configured.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(52)SE	This command was introduced.

**Usage Guidelines** After entering the **ip sla server twamp** command, you enter IP SLA TWAMP server configuration mode, and these configuration commands are available:

- **default:** sets a command to its defaults.
- **exit:** exits from IP SLA TWAMP server configuration mode.
- **no:** negates a command or resets to its defaults.
- **port *port-number*:** specifies the source port for TWAMP control traffic. Valid port numbers are from 1 to 65535.
- **timer inactivity *seconds*:** specifies the maximum time the session can be inactive before the session ends. The range is 1-6000 seconds. The default is 900 seconds.

For the TWAMP server and reflector to function, you must also configure a TWAMP control device, which serves as the client and session sender. These functions are not configured on a Cisco device.

**Examples** This example shows how to configure a switch as an IP SLA TWAMP server:

```
Switch(config)# ip sla server twamp
Switch(config-twamp-srvr)# port 862
Switch(config-twamp-srvr)# timer inactivity 540
```

Related Commands	Command	Description
	<b>ip sla responder</b>	Enables the Cisco IOS IP Service Level Agreements (SLAs) responder for general IP SLAs operations.
	<b>ip sla responder twamp</b>	Configures the switch as a Two-Way Active Measurement Protocol (TWAMP) responder.
	<b>show ip sla standards</b>	(Optional) Displays the IP SLAs standards configured on the switch.
	<b>show ip sla twamp connection {detail   requests}</b>	(Optional) Displays the current Cisco IOS IP Service Level Agreements (SLAs) Two-Way Active Measurement Protocol (TWAMP) connections.

# ip source binding

Use the **ip source binding** global configuration command to configure static IP source bindings on the switch. Use the **no** form of this command to delete static bindings.

**ip source binding** *mac-address* **vlan** *vlan-id* *ip-address* **interface** *interface-id*

**no source binding** *mac-address* **vlan** *vlan-id* *ip-address* **interface** *interface-id*

## Syntax Description

<i>mac-address</i>	Specify a MAC address.
<b>vlan</b> <i>vlan-id</i>	Specify a VLAN number. The range is from 1 to 4094.
<i>ip-address</i>	Specify an IP address.
<b>interface</b> <i>interface-id</i>	Specify an interface on which to add or delete an IP source binding.

## Defaults

No IP source bindings are configured.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

A static IP source binding entry has an IP address, its associated MAC address, and its associated VLAN number. The entry is based on the MAC address and the VLAN number. If you modify an entry by changing only the IP address, the switch updates the entry instead creating a new one.

## Examples

This example shows how to add a static IP source binding:

```
Switch(config)# ip source binding 0001.1234.1234 vlan 1 172.20.50.5 interface
gigabitethernet0/1
```

This example shows how to add a static binding and then modify the IP address for it:

```
Switch(config)# ip source binding 0001.1357.0007 vlan 1 172.20.50.25 interface
gigabitethernet0/1
Switch(config)# ip source binding 0001.1357.0007 vlan 1 172.20.50.30 interface
gigabitethernet0/1
```

You can verify your settings by entering the **show ip source binding** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">ip verify source</a>	Enables IP source guard on an interface.
	<a href="#">show ip source binding</a>	Displays the IP source bindings on the switch.
	<a href="#">show ip verify source</a>	Displays the IP source guard configuration on the switch or on a specific interface.

# ip ssh

Use the **ip ssh** global configuration command to configure the switch to run Secure Shell (SSH) Version 1 or SSH Version 2. Use the **no** form of this command to return to the default setting.

**ip ssh version [1 | 2]**

**no ip ssh version [1 | 2]**

This command is available only when your switch is running the cryptographic (encrypted) software image.

## Syntax Description

- |          |   |
|----------|---|
| <b>1</b> | (Optional) Configure the switch to run SSH Version 1 (SSHv1). |
| <b>2</b> | (Optional) Configure the switch to run SSH Version 2 (SSHv1). |

## Defaults

The default version is the latest SSH version supported by the SSH client.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

If you do not enter this command or if you do not specify a keyword, the SSH server selects the latest SSH version supported by the SSH client. For example, if the SSH client supports SSHv1 and SSHv2, the SSH server selects SSHv2.

The switch supports an SSHv1 or an SSHv2 server. It also supports an SSHv1 client. For more information about the SSH server and the SSH client, see the software configuration guide for this release.

A Rivest, Shamir, and Adelman (RSA) key pair generated by an SSHv1 server can be used by an SSHv2 server and the reverse.

## Examples

This example shows how to configure the switch to run SSH Version 2:

```
Switch(config)# ip ssh version 2
```

You can verify your settings by entering the **show ip ssh** or **show ssh** privileged EXEC command.

Related Commands	Command	Description
	<b>show ip ssh</b>	Displays if the SSH server is enabled and displays the version and configuration information for the SSH server. For syntax information, select <b>Cisco IOS Release 12.2 Configuration Guides and Command References &gt; Cisco IOS Security Command Reference, Release 12.2 &gt; Other Security Features &gt; Secure Shell Commands.</b>
	<b>show ssh</b>	Displays the status of the SSH server. For syntax information, select <b>Cisco IOS Release 12.2 Configuration Guides and Command References &gt; Cisco IOS Security Command Reference, Release 12.2 &gt; Other Security Features &gt; Secure Shell Commands.</b>



## ip sticky-arp (global configuration)

Use the **ip sticky-arp** global configuration command to enable sticky Address Resolution Protocol (ARP) on a switch virtual interface (SVI) that belongs to a private VLAN. Use the **no** form of this command to disable sticky ARP.

**ip sticky-arp**

**no ip sticky-arp**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Sticky ARP is enabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** Sticky ARP entries are those learned on private-VLAN SVIs. These entries do not age out. The **ip sticky-arp** global configuration command is supported only on SVIs belonging to private VLANs.

- When you configure a private VLAN, sticky ARP is enabled on the switch (the default). If you enter the **ip sticky-arp interface** configuration command, it does not take effect. If you enter the **no ip sticky-arp interface** configuration command, you do not disable sticky ARP on an interface.



**Note** We recommend that you use the **show arp** privileged EXEC command to display and verify private-VLAN interface ARP entries.

- If you disconnect the switch from a device and then connect it to another device with a different MAC address but with the same IP address, the ARP entry is not created, and this message appears:
 

```
*Mar 2 00:26:06.967: %IP-3-STCKYARPOVR: Attempt to overwrite Sticky ARP entry:
20.6.2.1, hw: 0000.0602.0001 by hw: 0000.0503.0001
```
- If a MAC address of a device changes, you must use the **no arp ip-address** global configuration command to manually remove the private-VLAN interface ARP entries.
- Use the **arp ip-address hardware-address type** global configuration command to add a private-VLAN ARP entry.

## ip sticky-arp (global configuration)

- Use the **no sticky-arp** global configuration command to disable sticky ARP on the switch.
- Use the **no sticky-arp** interface configuration command to disable sticky ARP on an interface when sticky ARP is disabled on the switch.

### Examples

To disable sticky ARP:

```
Switch(config)# no ip sticky-arp
```

You can verify your settings by using the **show arp** privileged EXEC command.

### Related Commands

Command	Description
<b>arp</b>	Adds a permanent entry in the ARP table. For syntax information, see the <b>Cisco IOS IP Addressing Services Command Reference, Release 12.4 &gt; ARP Commands</b> .
<b>show arp</b>	Displays the entries in the ARP table. For syntax information, see the <b>Cisco IOS IP Addressing Services Command Reference, Release 12.4 &gt; ARP Commands</b> .

## ip sticky-arp (interface configuration)

Use the **ip sticky-arp** interface configuration command to enable sticky Address Resolution Protocol (ARP) on a switch virtual interface (SVI) or a Layer 3 interface. Use the **no** form of this command to disable sticky ARP.

**ip sticky-arp**

**no ip sticky-arp**

### Syntax Description

This command has no arguments or keywords.

### Defaults

Sticky ARP is enabled on private-VLAN SVIs.

Sticky ARP is disabled on Layer 3 interfaces and normal SVIs.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

Sticky ARP entries are those learned on SVIs and Layer 3 interfaces. These entries do not age out.

The **ip sticky-arp** interface configuration command is only supported on

- Layer 3 interfaces
- SVIs belonging to normal VLANs
- SVIs belonging to private VLANs

On a Layer 3 interface or on an SVI belonging to a normal VLAN

- Use the **sticky-arp** interface configuration command to enable sticky ARP.
- Use the **no sticky-arp** interface configuration command to disable sticky ARP.

On private-VLAN SVIs

- When you configure a private VLAN, sticky ARP is enabled on the switch (the default).

If you enter the **ip sticky-arp interface** configuration command, it does not take effect.

If you enter the **no ip sticky-arp interface** configuration command, you do not disable sticky ARP on an interface.



#### Note

We recommend that you use the **show arp** privileged EXEC command to display and verify private-VLAN interface ARP entries.

## ip sticky-arp (interface configuration)

- If you disconnect the switch from a device and then connect it to another device with a different MAC address but with the same IP address, the ARP entry is not created, and this message appears:

```
*Mar 2 00:26:06.967: %IP-3-STCKYARPOVR: Attempt to overwrite Sticky ARP entry:
20.6.2.1, hw: 0000.0602.0001 by hw: 0000.0503.0001
```

- If a MAC address of a device changes, you must use the **no arp ip-address** global configuration command to manually remove the private-VLAN interface ARP entries.
- Use the **arp ip-address hardware-address type** global configuration command to add a private-VLAN ARP entry.
- Use the **no sticky-arp** global configuration command to disable sticky ARP on the switch.
- Use the **no sticky-arp** interface configuration command to disable sticky ARP on an interface.

### Examples

To enable sticky ARP on a normal SVI:

```
Switch(config-if)# ip sticky-arp
```

To disable sticky ARP on a Layer 3 interface or an SVI:

```
Switch(config-if)# no ip sticky-arp
```

You can verify your settings by using the **show arp** privileged EXEC command.

### Related Commands

Command	Description
<b>arp</b>	Adds a permanent entry in the ARP table. For syntax information, see the <b>Cisco IOS IP Addressing Services Command Reference, Release 12.4 &gt; ARP Commands</b> .
<b>show arp</b>	Displays the entries in the ARP table. For syntax information, see the <b>Cisco IOS IP Addressing Services Command Reference, Release 12.4 &gt; ARP Commands</b> .

## ip verify source

Use the **ip verify source** interface configuration command to enable IP source guard on an interface. Use the **no** form of this command to disable IP source guard.

**ip verify source** { **vlan dhcp-snooping** | **tracking** } [**port-security**]

**no ip verify source** { **vlan dhcp-snooping** | **tracking** } [**port-security**]

Syntax Description	
<b>vlan dhcp-snooping</b>	Enable IP source guard on an untrusted Layer 2 DHCP snooping interfaces.
<b>tracking</b>	Enable IP port security to learn static IP address learning on a port.
<b>port-security</b>	(Optional) Enable IP source guard with IP and MAC address filtering. If you do not enter the <b>port-security</b> keyword, IP address filtering is enabled.

**Defaults** IP source guard is disabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.
	12.2(52)SE	The <b>vlan dhcp-snooping</b> and <b>tracking</b> keywords were added.

**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.

To enable IP source guard with source IP and MAC address filtering, you must enable port security on the interface.

**Examples** This example shows how to enable IP source guard with source IP address filtering:

```
Switch(config-if)# ip verify source
```

This example shows how to enable IP source guard on VLANs 10 through 20 on a per-port basis:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10 20
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 10
```

```
Switch(config-if)# switchport trunk allowed vlan 11-20
Switch(config-if)# no ip dhcp snooping trust
Switch(config-if)# ip verify source vlan dhcp-snooping
Switch(config)# end
Switch# show ip verify source interface gigabitEthernet0/1
Interface  Filter-type  Filter-mode  IP-address  Mac-address  Vlan
-----
Gi0/1     ip-mac       active       10.0.0.1    -----
Gi0/1     ip-mac       active       deny-all    -----
Switch#
```

This example shows how to enable IP port security with IP-MAC filters on a Layer 2 access port:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitEthernet0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# end
```

Verify your settings by entering the **show ip verify source** privileged EXEC command.

#### Related Commands

Command	Description
<a href="#">ip device tracking maximum</a>	Enable IP port security binding tracking on a Layer 2 port.
<a href="#">ip dhcp snooping</a>	Globally enable DHCP snooping.
<a href="#">ip dhcp snooping limit rate</a>	Configure the number of the DHCP messages that an interface can receive per second.
<a href="#">ip dhcp snooping information option</a>	Enable DHCP option-82 data insertion.
<a href="#">ip dhcp snooping trust</a>	Enable DHCP snooping on a trusted VLAN.
<a href="#">ip source binding</a>	Configure static bindings on the switch.
<a href="#">show ip dhcp snooping</a>	Display the DHCP snooping configuration.
<a href="#">show ip dhcp snooping binding</a>	Display the DHCP snooping binding entries.
<a href="#">show ip verify source</a>	Display the IP source guard configuration on the switch or on a specific interface.

# ipv6 access-list

Use the **ipv6 access-list** global configuration command to define an IPv6 access list and to place the switch in IPv6 access list configuration mode. To remove the access list, use the **no** form of this command.

**ipv6 access-list** *access-list-name*

**no ipv6 access-list** *access-list-name*



## Note

This command is available only if the switch is running the metro IP access image and you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

## Syntax Description

<i>access-list-name</i>	Name of the IPv6 access list. Names cannot contain a space or quotation mark or begin with a number.
-------------------------	--

## Defaults

No IPv6 access list is defined.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(50)SE	This command was introduced.

## Usage Guidelines

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6 { default | routing | vlan }** global configuration command, and reload the switch.

The **ipv6 access-list** command is similar to the **ip access-list** command, but it is IPv6-specific.

IPv6 ACLs are defined by a unique name (IPv6 does not support numbered ACLs). An IPv4 ACL and an IPv6 ACL cannot share the same name.

See the [deny \(IPv6 access-list configuration\)](#) and [permit \(IPv6 access-list configuration\)](#) commands for more information on filtering IPv6 traffic based on IPv6 option headers and optional, upper-layer protocol-type information. See the “Examples” section for an example of a translated IPv6 ACL configuration.

Every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. The two **permit** conditions allow ICMPv6 neighbor discovery. To disallow ICMPv6 neighbor discovery and to deny **icmp any any nd-na** or **icmp any any nd-ns**, there must be an explicit **deny** entry in the ACL. For the implicit **deny ipv6 any any** statement to take effect, an IPv6 ACL must contain at least one entry.

The IPv6 neighbor discovery process uses the IPv6 network layer service; therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, uses a separate data-link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Use the **ipv6 traffic-filter** interface configuration command with the *access-list-name* argument to apply an IPv6 ACL to an IPv6 interface. You can apply inbound and outbound IPv6 ACLs to Layer 3 physical interfaces or to switch virtual interfaces for routed ACLs, but only inbound IPv6 ACLs to Layer 2 interfaces for port ACLs.

**Note**

An IPv6 ACL applied to an interface with the **ipv6 traffic-filter** command filters traffic that is forwarded by the switch and does not filter traffic generated by the switch.

**Examples**

This example puts the switch in IPv6 access list configuration mode, configures the IPv6 ACL named list2, and applies the ACL to outbound traffic on an interface. The first ACL entry prevents all packets from the network FE80:0:0:2::/64 (packets that have the link-local prefix FE80:0:0:2 as the first 64 bits of their source IPv6 address) from leaving the interface. The second entry in the ACL permits all other traffic to leave the interface. The second entry is necessary because an implicit deny-all condition is at the end of each IPv6 ACL.

```
Switch(config)# ipv6 access-list list2
Switch(config-ipv6-acl)# deny FE80:0:0:2::/64 any
Switch(config-ipv6-acl)# permit any any
Switch(config-ipv6-acl)# exit
Switch(config)# interface gigabitethernet0/3
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter list2 out
```

**Note**

IPv6 ACLs that rely on the implicit deny condition or specify a **deny any any** statement to filter traffic should contain **permit** statements for link-local addresses to avoid the filtering of protocol packets. Additionally IPv6 ACLs that use **deny** statements to filter traffic should also use a **permit any any** statement as the last statement in the list.

**Related Commands**

Command	Description
<a href="#">deny (IPv6 access-list configuration)</a>	Sets deny conditions for an IPv6 access list.
<a href="#">ipv6 traffic-filter</a>	Filters incoming or outgoing IPv6 traffic on an interface.
<a href="#">permit (IPv6 access-list configuration)</a>	Sets permit conditions for an IPv6 access list.
<a href="#">show ipv6 access-list</a>	Displays the contents of all current IPv6 access lists.



# ipv6 address dhcp

Use the **ipv6 address dhcp** interface configuration command to acquire an IPv6 address on an interface from the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server. To remove the address from the interface, use the **no** form of this command.

**ipv6 address dhcp [rapid-commit]**

**no ipv6 address dhcp [rapid-commit]**



## Note

This command is available only if the switch is running the metro IP access image and you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

Syntax Description	rapid-commit	(Optional) Allow two-message exchange method for address assignment.
--------------------	--------------	--

Defaults	No default is defined.
----------	------------------------

Command Modes	Interface configuration
---------------	-------------------------

Command History	Release	Modification
	12.2(50)SE	This command was introduced.

Usage Guidelines	<p>To configure the dual IPv4 and IPv6 template, enter the <b>sdm prefer dual-ipv4-and-ipv6 { default   routing   vlan }</b> global configuration command, and reload the switch.</p> <p>The <b>ipv6 address dhcp</b> interface configuration command allows any interface to dynamically learn its IPv6 address by using DHCP.</p> <p>The <b>rapid-commit</b> keyword enables the use of the two-message exchange for address allocation and other configuration. If it is enabled, the client includes the rapid-commit option in a solicit message.</p>
------------------	--

Examples	This example shows how to acquire an IPv6 address and to enable the rapid-commit option:
----------	--

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ipv6 address dhcp rapid-commit
```

You can verify your settings by using the **show ipv6 dhcp interface** privileged EXEC command.

Related Commands	Command	Description
	<b>show ipv6 dhcp interface</b>	Displays DHCPv6 interface information.

# ipv6 dhcp client request vendor

Use the **ipv6 dhcp client request** interface configuration command to configure an IPv6 client to request an option from a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server. To remove the request, use the **no** form of this command.

**ipv6 dhcp client request vendor**

**no ipv6 dhcp client request vendor**



## Note

This command is available only if the switch is running the metro IP access image and you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default is defined.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(50)SE	This command was introduced.

## Usage Guidelines

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6 {default | routing | vlan}** global configuration command, and reload the switch.

Use the **ipv6 dhcp client request vendor** interface configuration to request a vendor-specific option. When enabled, the command is verified only when an IPv6 address is acquired from DHCP. If you enter the command after the interface has an IPv6 address, the command does not take effect until the next time the client acquires an IPv6 address from DHCP.

## Examples

This example shows how to enable the request vendor-specific option.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ipv6 dhcp client request vendor-specific
```

## Related Commands

Command	Description
<a href="#">ipv6 address dhcp</a>	Acquires an IPv6 address on an interface from DHCP.

# ipv6 dhcp ping packets

Use the **ipv6 dhcp ping packets** global configuration command to specify the number of packets a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server sends to a pool address as part of a ping operation. To prevent the server from pinging pool addresses, use the **no** form of this command.

**ipv6 dhcp ping packets** *number*

**no ipv6 dhcp ping packets**



## Note

This command is available only if the switch is running the metro IP access image and you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

## Syntax Description

<i>number</i>	The number of ping packets sent before the address is assigned to a requesting client. The range is 0 to 10.
---------------	--

## Defaults

The default is 0.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(50)SE	This command was introduced.

## Usage Guidelines

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6 {default | vlan}** global configuration command, and reload the switch.

The DHCPv6 server pings a pool address before assigning it to a requesting client. An unanswered ping indicates that the address is not in use and the server assigns the address to the requesting client.

Setting the *number* argument to 0 turns off the DHCPv6 server ping operation.

## Examples

This example specifies two ping attempts by the DHCPv6 server before further ping attempts stop:

```
Switch(config)# ipv6 dhcp ping packets 2
```

## Related Commands

Command	Description
<a href="#">clear ipv6 dhcp conflict</a>	Clears an address conflict from the DHCPv6 server database.
<a href="#">show ipv6 dhcp conflict</a>	Displays address conflicts found by a DHCPv6 server or reported through a DECLINE message from a client.

# ipv6 dhcp pool

Use the **ipv6 dhcp pool** global configuration command to enter Dynamic Host Configuration Protocol for IPv6 (DHCPv6) pool configuration mode. Use the **no** form of this command to return to the default settings.

**ipv6 dhcp pool** *poolname*

**no ipv6 dhcp pool** *poolname*



## Note

This command is available only if the switch is running the metro IP access image and you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

## Syntax Description

<i>poolname</i>	User-defined name for the DHCPv6 pool. The pool name can be a symbolic string (such as <i>Engineering</i> ) or an integer (such as 0).
-----------------	--

## Defaults

No default is defined.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(50)SE	This command was introduced.

## Usage Guidelines

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6 {default | vlan}** global configuration command, and reload the switch.

DHCPv6 pool configuration mode commands:

- **address prefix** *IPv6-prefix*: sets an address prefix for address assignment. This address must be in hexadecimal, using 16-bit values between colons.
- **lifetime** *t1 t2*: sets a *valid* and a *preferred* time interval (in seconds) for the IPv6 address. The range is 5 to 4294967295 seconds. The valid default is 2 days. The preferred default is 1 day. The valid lifetime must be greater than or equal to the preferred lifetime. Specify **infinite** for no time interval.
- **link-address** *IPv6-prefix*: sets a link-address IPv6 prefix. When an address on the incoming interface or a link-address in the packet matches the specified IPv6-prefix, the server uses the configuration information pool. This address must be in hexadecimal, using 16-bit values between colons.

- **vendor-specific**: enables the DHCPv6 vendor-specific configuration mode with these configuration commands:
  - *vendor-id*: enter a vendor-specific identification number. This number is the vendor IANA Private Enterprise Number. The range is 1 to 4294967295.
  - **suboption number**: sets vendor-specific suboption number. The range is 1 to 65535. Enter an IPv6 address, ASCII text, or a hexadecimal string as defined by the suboption parameters.

After you create the DHCPv6 configuration information pool, use the **ipv6 dhcp server** interface configuration command to associate the pool with a server on an interface. However, if you do not configure an information pool, you still need to use the **ipv6 dhcp server** interface configuration command to enable the DHCPv6 server function on an interface.

When you associate a DHCPv6 pool with an interface, only that pool services requests on the associated interface. The pool also services other interfaces. If you do not associate a DHCPv6 pool with an interface, it can service requests on any interface.

Not using any IPv6 address prefix means that the pool only returns configured options.

The **link-address** keyword allows matching of a link-address without necessarily allocating an address. You can match the pool from multiple relays by using multiple link-address configuration commands inside a pool.

Because a longest match is performed on either the address pool information or the link information, you can configure one pool to allocate addresses and another pool on a subprefix that only returns configured options.

## Examples

This example shows how to configure a pool called *engineering* with an IPv6 address prefix:

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool engineering
Switch(config-dhcpv6)# address prefix 2001:1000::0/64
Switch(config-dhcpv6)# end
```

This example shows how to configure a pool called *testgroup* with three link-address prefixes and an IPv6 address prefix:

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool testgroup
Switch(config-dhcpv6)# link-address 2001:1001::0/64
Switch(config-dhcpv6)# link-address 2001:1002::0/64
Switch(config-dhcpv6)# link-address 2001:2000::0/48
Switch(config-dhcpv6)# address prefix 2001:1003::0/64
Switch(config-dhcpv6)# end
```

This example shows how to configure a pool called *350* with vendor-specific options:

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool 350
Switch(config-dhcpv6)# vendor-specific 9
Switch(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Switch(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Switch(config-dhcpv6-vs)# end
```

■ **ipv6 dhcp pool****Related Commands**

<b>Command</b>	<b>Description</b>
<b>ipv6 dhcp server</b>	Enables DHCPv6 service on an interface.
<b>show ipv6 dhcp pool</b>	Displays DHCPv6 configuration pool information.

# ipv6 dhcp server

Use the **ipv6 dhcp server** interface configuration command to enable Dynamic Host Configuration Protocol for IPv6 (DHCPv6) service on an interface. To disable DHCPv6 service on an interface, use the **no** form of this command.

```
ipv6 dhcp server [poolname | automatic] [allow-hint] [rapid-commit] [preference value]
```

```
no ipv6 dhcp server
```



### Note

This command is available only if the is running the metro IP access image and you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

### Syntax Description

<i>poolname</i>	(Optional) User-defined name for the IPv6 DHCP pool. The pool name can be a symbolic string (such as <i>Engineering</i> ) or an integer (such as 0).
<b>automatic</b>	(Optional) Enable the server to automatically determine which pool to use when allocating addresses for a client.
<b>allow-hint</b>	(Optional) Specify whether the server should consider client suggestions in the SOLICIT message. By default, the server ignores client suggestions.
<b>preference value</b>	(Optional) The preference value carried in the preference option in the advertise message sent by the server. The range is from 0 to 255. The default is 0.
<b>rapid-commit</b>	(Optional) Allow two-message exchange method.

### Defaults

By default, no DHCPv6 packets are serviced on the interface.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(50)SE	The <b>automatic</b> keyword was added to the command.

### Usage Guidelines

The **ipv6 dhcp server** interface configuration command enables DHCPv6 service on a specified interface.

If you enter the **automatic** keyword, the system automatically determine which pool to use when allocating addresses for a client. When the server receives an IPv6 DHCP packet, the server determines if it was received from a DHCP relay or if it was directly received from the client. If the packet was received from a relay, the server verifies the link-address field inside the packet associated with the first relay that is closest to the client. The server matches this link-address against all address prefix and link-address configurations in IPv6 DHCP pools to find the longest prefix match. The server selects the pool associated with the longest match.

If the packet was received directly from the client, the server performs this same matching, but it uses all the IPv6 addresses configured on the incoming interface when performing the match. Once again, the server selects the longest prefix match.

If you enter the **allow-hint** keyword, the server allocates a valid client-suggested address in the solicit and request messages. The prefix address is valid if it is in the associated local prefix address pool and it is not assigned to a device. If the **allow-hint** keyword is not specified, the server ignores the client hint, and an address is allocated from the free list in the pool.

If you configure the **preference** keyword with a value other than 0, the server adds a preference option to carry the preference value for the advertise messages. This action affects the selection of a server by the client. Any advertise message that does not include a preference option is considered to have a preference value of 0. If the client receives an advertise message with a preference value of 255, the client immediately sends a request message to the server from which the message was received.

Entering the **rapid-commit** keyword enables the use of the two-message exchange.

The DHCPv6 client, server, and relay functions are mutually exclusive on an interface. When one of these functions is already enabled and you try to configure a different function on the same interface, the switch returns one of these messages:

```
Interface is in DHCP client mode
Interface is in DHCP server mode
Interface is in DHCP relay mode
```

### Examples

This example enables DHCPv6 for the pool named testgroup:

```
Switch(config-if)# ipv6 dhcp server testgroup
```

### Related Commands

Command	Description
<b>ipv6 dhcp pool</b>	Configures a DHCPv6 pool and enters DHCPv6 pool configuration mode.
<b>show ipv6 dhcp interface</b>	Displays DHCPv6 interface information.



# ipv6 mld snooping

Use the **ipv6 mld snooping** global configuration command without keywords to enable IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping globally or on the specified VLAN. Use the **no** form of this command to disable MLD snooping on the switch or switch stack or the VLAN.

```
ipv6 mld snooping [vlan vlan-id]
```

```
no ipv6 mld snooping [vlan vlan-id]
```



## Note

This command is available only if the switch is running the metro IP access image and you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

## Syntax Description

<b>vlan</b> <i>vlan-id</i>	(Optional) Enable or disable IPv6 MLD snooping on the specified VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.
----------------------------	--

## Defaults

MLD snooping is globally disabled on the switch.

MLD snooping is enabled on all VLANs. However, MLD snooping must be globally enabled before VLAN snooping will take place.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(52)SE	This command was introduced.

## Usage Guidelines

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6** global configuration command and reload the switch.

When MLD snooping is globally disabled, it is disabled on all the existing VLAN interfaces. When you globally enable MLD snooping, it is enabled on all VLAN interfaces that are in the default state (enabled). VLAN configuration will override global configuration on interfaces on which MLD snooping has been disabled.

If MLD snooping is globally disabled, you cannot enable it on a VLAN. If MLD snooping is globally enabled, you can disable it on individual VLANs.

When the IPv6 multicast router is a Catalyst 6500 switch and you are using extended VLANs (in the range 1006 to 4094), IPv6 MLD snooping must be enabled on the extended VLAN on the Catalyst 6500 switch in order for the switch to receive queries on the VLAN. For normal-range VLANs (1 to 1005), it is not necessary to enable IPv6 MLD snooping on the VLAN on the Catalyst 6500 switch.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

**Examples**

This example shows how to globally enable MLD snooping:

```
Switch(config)# ipv6 mld snooping
```

This example shows how to disable MLD snooping on a VLAN:

```
Switch(config)# no ipv6 mld snooping vlan 11
```

You can verify your settings by entering the **show ipv6 mld snooping** user EXEC command.

**Related Commands**

Command	Description
<a href="#">sdm prefer</a>	Configures an SDM template to optimize system resources based on how the switch is being used.
<b>show ipv6 mld snooping</b>	Displays MLD snooping configuration.

## ipv6 mld snooping last-listener-query-count

Use the **ipv6 mld snooping last-listener-query-count** global configuration command to configure IP version 6 (IPv6) Multicast Listener Discovery Multicast Address Specific Queries (MASQs) or that will be sent before aging out a client. Use the **no** form of this command to reset the query count to the default settings.

```
ipv6 mld snooping [vlan vlan-id] last-listener-query-count integer_value
```

```
no ipv6 mld snooping [vlan vlan-id] last-listener-query-count
```



### Note

This command is available only if the switch is running the metro IP access image and you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

### Syntax Description

<b>vlan <i>vlan-id</i></b>	(Optional) Configure last-listener query count on the specified VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.
<b><i>integer_value</i></b>	The range is 1 to 7.

### Command Default

The default global count is 2.

The default VLAN count is 0 (the global count is used).

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(52)SE	This command was introduced.

### Usage Guidelines

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6** global configuration command and reload the switch.

In MLD snooping, the IPv6 multicast router periodically sends out queries to hosts belonging to the multicast group. If a host wants to leave a multicast group, it can silently leave or it can respond to the query with a Multicast Listener Done message (equivalent to an IGMP Leave message). When Immediate Leave is not configured (which it should not be if multiple clients for a group exist on the same port), the configured last-listener query count determines the number of MASQs that are sent before an MLD client is aged out.

When the last-listener query count is set for a VLAN, this count overrides the value configured globally. When the VLAN count is not configured (set to the default of 0), the global count is used.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

**Examples**

This example shows how to globally set the last-listener query count:

```
Switch(config)# ipv6 mld snooping last-listener-query-count 1
```

This example shows how to set the last-listener query count for VLAN 10:

```
Switch(config)# ipv6 mld snooping vlan 10 last-listener-query-count 3
```

You can verify your settings by entering the **show ipv6 mld snooping [vlan *vlan-id*]** user EXEC command.

**Related Commands**

Command	Description
<a href="#">ipv6 mld snooping last-listener-query-interval</a>	Sets IPv6 MLD snooping last-listener query interval.
<a href="#">sdm prefer</a>	Configures an SDM template to optimize system resources based on how the switch is being used.
<b>show ipv6 mld snooping querier</b>	Displays MLD snooping configuration.

## ipv6 mld snooping last-listener-query-interval

Use the **ipv6 mld snooping last-listener-query-interval** global configuration command to configure IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping last-listener query interval on the switch or on a VLAN. This time interval is the maximum time that a multicast router waits after issuing a Multicast Address Specific Query (MASQ) before deleting a port from the multicast group. Use the **no** form of this command to reset the query time to the default settings.

**ipv6 mld snooping** [**vlan** *vlan-id*] **last-listener-query-interval** *integer\_value*

**no ipv6 mld snooping** [**vlan** *vlan-id*] **last-listener-query-interval**



### Note

This command is available only if the switch is running the metro IP access image and you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

### Syntax Description

<b>vlan</b> <i>vlan-id</i>	(Optional) Configure last-listener query interval on the specified VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.
<i>integer_value</i>	Set the time period (in thousands of a second) that a multicast router to wait after issuing a MASQ before deleting a port from the multicast group. The range is 100 to 32,768. The default is 1000 (1 second),

### Command Default

The default global query interval (maximum response time) is 1000 (1 second).  
The default VLAN query interval (maximum response time) is 0 (the global count is used).

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(52)SE	This command was introduced.

### Usage Guidelines

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6** global configuration command and reload the switch.

In MLD snooping, when the IPv6 multicast router receives an MLD leave message, it sends out queries to hosts belonging to the multicast group. If there are no responses from a port to a MASQ for a length of time, the router deletes the port from the membership database of the multicast address. The last listener query interval is the maximum time that the router waits before deleting a nonresponsive port from the multicast group.

When a VLAN query interval is set, this overrides the global query interval. When the VLAN interval is set at 0, the global value is used.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

**Examples**

This example shows how to globally set the last-listener query interval to 2 seconds:

```
Switch(config)# ipv6 mld snooping last-listener-query-interval 2000
```

This example shows how to set the last-listener query interval for VLAN 1 to 5.5 seconds:

```
Switch(config)# ipv6 mld snooping vlan 1 last-listener-query-interval 5500
```

You can verify your settings by entering the **show ipv6 MLD snooping [vlan *vlan-id*]** user EXEC command.

**Related Commands**

Command	Description
<a href="#">ipv6 mld snooping last-listener-query-count</a>	Sets IPv6 MLD snooping last-listener query count.
<a href="#">sdm prefer</a>	Configures an SDM template to optimize system resources based on how the switch is being used.
<b>show ipv6 mld snooping querier</b>	Sets IPv6 MLD snooping last-listener query interval.

# ipv6 mld snooping listener-message-suppression

Use the **ipv6 mld snooping listener-message-suppression** global configuration command to enable IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping listener message suppression. Use the **no** form of this command to disable MLD snooping listener message suppression.

**ipv6 mld snooping listener-message-suppression**

**no ipv6 mld snooping listener-message-suppression**



## Note

This command is available only if the switch is running the metro IP access image and you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

## Command Default

The default is for MLD snooping listener message suppression to be disabled.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(52)SE	This command was introduced.

## Usage Guidelines

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6** global configuration command and reload the switch.

MLD snooping listener message suppression is equivalent to IGMP snooping report suppression. When enabled, received MLDv1 reports to a group are forwarded to IPv6 multicast routers only once in every report-forward time. This prevents the forwarding of duplicate reports.

## Examples

This example shows how to enable MLD snooping listener-message-suppression:

```
Switch(config)# ipv6 mld snooping listener-message-suppression
```

This example shows how to disable MLD snooping listener-message-suppression:

```
Switch(config)# no ipv6 mld snooping listener-message-suppression
```

You can verify your settings by entering the **show ipv6 mld snooping [vlan vlan-id]** user EXEC command.

## Related Commands

Command	Description
<a href="#">ipv6 mld snooping</a>	Enables IPv6 MLD snooping.
<a href="#">sdm prefer</a>	Configures an SDM template to optimize system resources based on how the switch is being used.
<b>show ipv6 mld snooping</b>	Displays MLD snooping configuration.

## ipv6 mld snooping robustness-variable

Use the **ipv6 mld snooping robustness-variable** global configuration command to configure the number of IP version 6 (IPv6) Multicast Listener Discovery (MLD) queries that the switch sends before deleting a listener that does not respond, or enter a VLAN ID to configure on a per-VLAN basis. Use the **no** form of this command to reset the variable to the default settings.

**ipv6 mld snooping** [*vlan vlan-id*] **robustness-variable** *integer\_value*

**no ipv6 mld snooping** [*vlan vlan-id*] **robustness-variable**



### Note

This command is available only if the switch is running the metro IP access image and you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

### Syntax Description

<b>vlan</b> <i>vlan-id</i>	(Optional) Configure the robustness variable on the specified VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.
<i>integer_value</i>	The range is 1 to 3.

### Command Default

The default global robustness variable (number of queries before deleting a listener) is 2.

The default VLAN robustness variable (number of queries before aging out a multicast address) is 0, which means that the system uses the global robustness variable for aging out the listener.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(52)SE	This command was introduced.

### Usage Guidelines

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6** global configuration command and reload the switch.

Robustness is measured in terms of the number of MLDv1 queries sent with no response before a port is removed from a multicast group. A port is deleted when there are no MLDv1 reports received for the configured number of MLDv1 queries. The global value determines the number of queries that the switch waits before deleting a listener that does not respond and applies to all VLANs that do not have a VLAN value set.

The robustness value configured for a VLAN overrides the global value. If the VLAN robustness value is 0 (the default), the global value is used.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.



**Examples**

This example shows how to configure the global robustness variable so that the switch sends out three queries before it deletes a listener port that does not respond:

```
Switch(config)# ipv6 mld snooping robustness-variable 3
```

This example shows how to configure the robustness variable for VLAN 1. This value overrides the global configuration for the VLAN:

```
Switch(config)# ipv6 mld snooping vlan 1 robustness-variable 1
```

You can verify your settings by entering the **show ipv6 MLD snooping [vlan *vlan-id*]** user EXEC command.

**Related Commands**

Command	Description
<a href="#">ipv6 mld snooping last-listener-query-count</a>	Sets IPv6 MLD snooping last-listener query count.
<a href="#">sdm prefer</a>	Configures an SDM template to optimize system resources based on how the switch is being used.
<b>show ipv6 mld snooping</b>	Displays MLD snooping configuration.

## ipv6 mld snooping tcn

Use the **ipv6 mld snooping tcn** global configuration commands to configure IP version 6 (IPv6) Multicast Listener Discovery (MLD) Topology Change Notifications (TCNs). Use the **no** form of the commands to reset the default settings.

**ipv6 mld snooping tcn** { **flood query count** *integer\_value* | **query solicit** }

**no ipv6 mld snooping tcn** { **flood query count** *integer\_value* | **query solicit** }



### Note

This command is available only if the switch is running the metro IP access image and you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

### Syntax Description

<b>flood query count</b> <i>integer_value</i>	Set the flood query count, which is the number of queries that are sent before forwarding multicast data to only those ports requesting to receive it. The range is 1 to 10.
<b>query solicit</b>	Enable soliciting of TCN queries.

### Command Default

TCN query soliciting is disabled.  
When enabled, the default flood query count is 2.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(52)SE	This command was introduced.

### Usage Guidelines

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6** global configuration command and reload the switch.

### Examples

This example shows how to enable TCN query soliciting:

```
Switch(config)# ipv6 mld snooping tcn query solicit.
```

This example shows how to set the flood query count to 5:

```
Switch(config)# ipv6 mld snooping tcn flood query count 5.
```

You can verify your settings by entering the **show ipv6 MLD snooping [vlan vlan-id]** user EXEC command.

Related Commands	Command	Description
	<a href="#">sdm prefer</a>	Configures an SDM template to optimize system resources based on how the switch is being used.
	show ipv6 mld snooping	Displays MLD snooping configuration.

## ipv6 mld snooping vlan

Use the **ipv6 mld snooping vlan** global configuration command to configure IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping parameters on the VLAN interface. Use the **no** form of this command to reset the parameters to the default settings.

```
ipv6 mld snooping vlan vlan-id [immediate-leave | mrouter interface interface-id | static
ipv6-multicast-address interface interface-id]
```

```
no ipv6 mld snooping vlan vlan-id [immediate-leave | mrouter interface interface-id | static
ip-address interface interface-id]
```



### Note

This command is available only if the switch is running the metro IP access image and you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

### Syntax Description

<b>vlan</b> <i>vlan-id</i>	Specify a VLAN number. The range is 1 to 1001 and 1006 to 4094.
<b>immediate-leave</b>	(Optional) Enable MLD Immediate-Leave processing on a VLAN interface. Use the <b>no</b> form of the command to disable the Immediate Leave feature on the interface.
<b>mrouter interface</b>	(Optional) Configure a multicast router port. The <b>no</b> form of the command removes the configuration.
<b>static</b> <i>ipv6-multicast-address</i>	(Optional) Configure a multicast group with the specified IPv6 multicast address.
<b>interface</b> <i>interface-id</i>	Add a Layer 2 port to the group. The mrouter or static interface can be a physical port or a <b>port-channel</b> interface in the range of 1 to 48.

### Command Default

MLD snooping Immediate-Leave processing is disabled.  
By default, there are no static IPv6 multicast groups.  
By default, there are no multicast router ports.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(52)SE	This command was introduced.

### Usage Guidelines

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6** global configuration command and reload the switch.

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

The **static** keyword is used for configuring the MLD member ports statically.

The configuration and the static ports and groups are saved in NVRAM.

When the IPv6 multicast router is a Catalyst 6500 switch and you are using extended VLANs (in the range 1006 to 4094), IPv6 MLD snooping must be enabled on the extended VLAN on the Catalyst 6500 switch in order for the switch to receive queries on the VLAN. For normal-range VLANs (1 to 1005), it is not necessary to enable IPv6 MLD snooping on the VLAN on the Catalyst 6500 switch.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

### Examples

This example shows how to enable MLD Immediate-Leave processing on VLAN 1:

```
Switch(config)# ipv6 mld snooping vlan 1 immediate-leave
```

This example shows how to disable MLD Immediate-Leave processing on VLAN 1:

```
Switch(config)# no ipv6 mld snooping vlan 1 immediate-leave
```

This example shows how to configure a port as a multicast router port:

```
Switch(config)# ipv6 mld snooping vlan 1 mrouter interface gigabitethernet1/01/2
```

This example shows how to configure a static multicast group:

```
Switch(config)# ipv6 mld snooping vlan 2 static FF12::34 interface gigabitethernet1/01/2
```

You can verify your settings by entering the **show ipv6 mld snooping vlan *vlan-id*** user EXEC command.

### Related Commands

Command	Description
<a href="#">ipv6 mld snooping</a>	Enables IPv6 MLD snooping.
<a href="#">ipv6 mld snooping vlan</a>	Configures IPv6 MLD snooping on the VLAN.
<a href="#">sdm prefer</a>	Configures an SDM template to optimize system resources based on how the switch is being used.
<a href="#">show ipv6 mld snooping</a>	Displays IPv6 MLD snooping configuration.

## ipv6 traffic-filter

Use the **ipv6 traffic-filter** interface configuration command to filter IPv6 traffic on an interface. Use the **no** form of this command to disable the filtering of IPv6 traffic on an interface.

**ipv6 traffic-filter** *access-list-name* {**in** | **out**}

**no ipv6 traffic-filter** {**in** | **out**}



### Note

This command is available only if you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

### Syntax Description

<i>access-list-name</i>	Specify an IPv6 access name.
<b>in</b>	Specify incoming IPv6 traffic.
<b>out</b>	Specify outgoing IPv6 traffic.
<b>Note</b>	The <b>out</b> keyword is not supported for Layer 2 interfaces (port ACLs). The <b>out</b> keyword is supported for Layer 3 interfaces only when the switch is running the metro IP access image.

### Defaults

Filtering of IPv6 traffic on an interface is not configured.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(50)SE	This command was introduced.

### Usage Guidelines

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6 {default | routing | vlan}** global configuration command, and reload the switch.

You can use the **ipv6 traffic-filter** command on physical interfaces (Layer 2 or Layer 3 ports), Layer 3 port channels, or switch virtual interfaces (SVIs).

If the switch is running the metro IP access image, you can apply an ACL to outbound or inbound traffic on Layer 3 interfaces (router ACLs), or to inbound traffic on Layer 2 interfaces (port ACLs). If the switch is running the metro access image, you can apply ACLs only to inbound management traffic on Layer 2 interfaces. These images do not support router ACLs.

If *any* port ACL (IPv4, IPv6, or MAC) is applied to an interface, that port ACL filters packets, and any router ACLs attached to the SVI of the port VLAN are ignored.

**Examples**

This example filters inbound IPv6 traffic on an IPv6-configured interface as defined by the access list named *cisco*:

```
Switch (config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter cisco in
```

**Related Commands**

Command	Description
<a href="#">ipv6 access-list</a>	Defines an IPv6 access list and sets deny or permit conditions for the defined access list.
<a href="#">show ipv6 access-list</a>	Displays the contents of all current IPv6 access lists.
<a href="#">show ipv6 interface</a>	Displays the usability status of interfaces configured for IPv6.

## l2protocol-tunnel

To enable tunneling of Layer 2 protocols on an access or 802.1Q tunnel port, use the **l2protocol-tunnel** command in interface configuration mode. You can enable tunneling for Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), Spanning Tree Protocol (STP), or VLAN Trunking Protocol (VTP) packets, or configure the maximum number of incoming Layer 2 protocol packets to be received before the port is disabled or the interface drops packets. You can also enable point-to-point tunneling for Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), or UniDirectional Link Detection (UDLD) packets. To disable tunneling on the interface, to return to having no shutdown threshold, or to return to having no drop threshold, use the **no** form of this command.

```
l2protocol-tunnel [cdp | lldp | stp | vtp] [point-to-point [pagp | lacp | udld]] |
  [shutdown-threshold [cdp | lldp | stp | vtp] [point-to-point [pagp | lacp | udld]] value] |
  [drop-threshold [cdp | lldp | stp | vtp] [point-to-point [pagp | lacp | udld]] value]

no l2protocol-tunnel [cdp | lldp | stp | vtp] [point-to-point [pagp | lacp | udld]] |
  [shutdown-threshold [cdp | lldp | stp | vtp] [point-to-point [pagp | lacp | udld]] value] |
  [drop-threshold [cdp | lldp | stp | vtp] [point-to-point [pagp | lacp | udld]] value]
```

### Syntax Description

<b>l2protocol-tunnel</b>	Enable point-to-multipoint tunneling of CDP, STP, and VTP packets.
<b>cdp</b>	(Optional) Enable tunneling of CDP, specify a shutdown threshold for CDP, or specify a drop threshold for CDP.
<b>lldp</b>	(Optional) Enables tunneling of LLDP, specify a shutdown threshold for LLDP, or specify a drop threshold for LLDP.
<b>stp</b>	(Optional) Enable tunneling of STP, specify a shutdown threshold for STP, or specify a drop threshold for STP.
<b>vtp</b>	(Optional) Enable tunneling or VTP, specify a shutdown threshold for VTP, or specify a drop threshold for VTP.
<b>drop-threshold</b>	(Optional) Set a drop threshold for the maximum rate of Layer 2 protocol packets per second to be received before an interface drops packets.
<b>point-to-point</b>	(Optional) Enable point-to point tunneling of PAgP, LACP, and UDLD packets.
<b>pagp</b>	(Optional) Enable point-to-point tunneling of PAgP, specify a shutdown threshold for PAgP, or specify a drop threshold for PAgP.
<b>lacp</b>	(Optional) Enable point-to-point tunneling of LACP, specify a shutdown threshold for LACP, or specify a drop threshold for LACP.
<b>udld</b>	(Optional) Enable point-to-point tunneling of UDLD, specify a shutdown threshold for UDLD, or specify a drop threshold for UDLD.
<b>shutdown-threshold</b>	(Optional) Set a shutdown threshold for the maximum rate of Layer 2 protocol packets per second to be received before an interface is shut down.
<i>value</i>	Specify a threshold in packets per second to be received for encapsulation before the interface shuts down, or specify the threshold before the interface drops packets. The range is 1 to 4096. The default is no threshold.

### Defaults

The default is that no Layer 2 protocol packets are tunneled. If you enter the command with no keyword, tunneling is enabled for all CDP, LLDP, STP, and VTP packets.



If you enable point-to-point protocol tunneling with no keyword is entered, tunneling is enabled for all three point-to-point protocols.

The default is no shutdown threshold for the number of Layer 2 protocol packets.

The default is no drop threshold for the number of Layer 2 protocol packets.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.
	12.2(58)SE	Support was added for LLDP tunneling.

**Usage Guidelines** You must enter this command, with or without protocol types, to tunnel Layer 2 packets.

If you enter this command for a port channel, all ports in the channel must have the same configuration.

Layer 2 protocol tunneling across a service-provider network ensures that Layer 2 information is propagated across the network to all customer locations. When protocol tunneling is enabled, protocol packets are encapsulated with a well-known Cisco multicast address for transmission across the network. When the packets reach their destination, the well-known MAC address is replaced by the Layer 2 protocol MAC address.

You can enable Layer 2 protocol tunneling individually for CDP, LLDP, STP, VTP, or for all these protocols.



**Note**

The switch does not support VTP. CDP and STP are enabled by default network node interfaces (NNIs) and disabled by default but can be enabled on enhanced network interfaces (ENIs). User network interfaces (UNIs) do not support any of these protocols.

In a service-provider network, you can use Layer 2 protocol tunneling to enhance the creation of EtherChannels by emulating a point-to-point network topology. When protocol tunneling is enabled on the service-provider switch for PAgP or LACP, remote customer switches receive the protocol data units (PDUs) and can negotiate automatic creation of EtherChannels.



**Note**

Only NNIs and ENIs support PAgP and LACP.

To enable tunneling of PAgP, LACP, and UDLD packets, you must have a point-to-point network topology. To decrease the link-down detection time, you should also enable UDLD on the interface when you enable tunneling of PAgP or LACP packets.

You can enable point-to-point protocol tunneling for PAgP, LACP, and UDLD individually or for all three protocols.



**Caution**

PAgP, LACP, and UDLD tunneling is only intended to emulate a point-to-point topology. An erroneous configuration that sends tunneled packets to many ports could lead to a network failure.

Enter the **shutdown-threshold** keyword to control the number of protocol packets per second that are received on an interface before it shuts down. When no protocol option is specified with the keyword, the threshold is applied to each of the tunneled Layer 2 protocol types. If you also set a drop threshold on the interface, the shutdown-threshold value must be greater than or equal to the drop-threshold value.

When the shutdown threshold is reached, the interface is error-disabled. If you enable error recovery by entering the **errdisable recovery cause l2ptguard** global configuration command, the interface is brought out of the error-disabled state and allowed to retry the operation again when all the causes have timed out. If the error recovery mechanism is not enabled for **l2ptguard**, the interface stays in the error-disabled state until you enter the **shutdown** and **no shutdown** interface configuration commands.

Enter the **drop-threshold** keyword to control the number of protocol packets per second that are received on an interface before it drops packets. When no protocol option is specified with a keyword, the threshold is applied to each of the tunneled Layer 2 protocol types. If you also set a shutdown threshold on the interface, the drop-threshold value must be less than or equal to the shutdown-threshold value.

When the drop threshold is reached, the interface drops Layer 2 protocol packets until the rate at which they are received is below the drop threshold.

The configuration is saved in NVRAM.

**Note**

For more information about Layer 2 protocol tunneling, see the software configuration guide for this release.

**Examples**

This example shows how to enable protocol tunneling for CDP packets and to configure the shutdown threshold as 50 packets per second:

```
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)# l2protocol-tunnel shutdown-threshold cdp 50
```

This example shows how to enable protocol tunneling for STP packets and to configure the drop threshold as 400 packets per second:

```
Switch(config-if)# l2protocol-tunnel stp
Switch(config-if)# l2protocol-tunnel drop-threshold stp 400
```

This example shows how to enable point-to-point protocol tunneling for PAgP and UDLD packets and to configure the PAgP drop threshold as 1000 packets per second:

```
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
```

**Related Commands**

Command	Description
<a href="#">l2protocol-tunnel cos</a>	Configures a class of service (CoS) value for all tunneled Layer 2 protocol packets.
<a href="#">show errdisable recovery</a>	Displays errdisable recovery timer information.
<a href="#">show l2protocol-tunnel</a>	Displays information about ports configured for Layer 2 protocol tunneling, including port, protocol, CoS, and threshold.

# l2protocol-tunnel cos

Use the **l2protocol-tunnel cos** global configuration command to configure class of service (CoS) value for all tunneled Layer 2 protocol packets. Use the **no** form of this command to return to the default setting.

**l2protocol-tunnel cos** *value*

**no l2protocol-tunnel cos**

## Syntax Description

<i>value</i>	Specify CoS priority value for tunneled Layer 2 protocol packets. If a CoS value is configured for data packets for the interface, the default is to use this CoS value. If no CoS value is configured for the interface, the default is 5. The range is 0 to 7, with 7 being the highest priority.
--------------	---

## Defaults

The default is to use the CoS value configured for data on the interface. If no CoS value is configured, the default is 5 for all tunneled Layer 2 protocol packets.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

When enabled, the tunneled Layer 2 protocol packets use this CoS value.  
The value is saved in NVRAM.

## Examples

This example shows how to configure a Layer-2 protocol-tunnel CoS value of 7:

```
Switch(config)# l2protocol-tunnel cos 7
```

## Related Commands

Command	Description
<a href="#">show l2protocol-tunnel</a>	Displays information about ports configured for Layer 2 protocol tunneling, including CoS.

# lax port-priority

Use the **lax port-priority** interface configuration command to configure the port priority for the Link Aggregation Control Protocol (LACP). Use the **no** form of this command to return to the default setting.

**lax port-priority** *priority*

**no lax port-priority**



## Note

LACP is available only on network node interfaces (NNIs) and enhanced network interfaces (ENIs).

## Syntax Description

<i>priority</i>	Port priority for LACP. The range is 1 to 65535.
-----------------	--

## Defaults

The default is 32768.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The **lax 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. This command takes effect only on EtherChannel ports that are already configured for LACP. If the interface is a user network interface (UNI), you must use the **port-type nni** or **port-type eni** interface configuration command to change the interface to an NNI or ENI before configuring **lax port-priority**.

In priority comparisons, numerically *lower* values have *higher* priority. The switch uses the priority to decide which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from being active. If two or more ports have the same LACP port priority (for example, they are configured with the default setting of 65535), an internal value for the port number determines the priority.



## Note

The LACP port priorities are only effective if the ports are on the switch that controls the LACP link. See the **lax system-priority** global configuration command for information about determining which switch controls the link.

Use the **show lax internal** privileged EXEC command to display LACP port priorities and internal port number values.

For information about configuring LACP on physical ports, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

---

**Examples**

This example shows how to configure the LACP port priority on a port:

```
Switch(config)# interface gigabitethernet0/1  
Switch(config-if)# lACP port-priority 1000
```

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

---

**Related Commands**

Command	Description
<a href="#">channel-group</a>	Assigns an Ethernet port to an EtherChannel group.
<a href="#">lACP system-priority</a>	Configures the LACP system priority.
<a href="#">show lACP</a> [ <i>channel-group-number</i> ] <b>internal</b>	Displays internal information for all channel groups or for the specified channel group.

# lacp system-priority

Use the **lacp system-priority** global configuration command to configure the system priority for the Link Aggregation Control Protocol (LACP). Use the **no** form of this command to return to the default setting.

**lacp system-priority** *priority*

**no lacp system-priority**



## Note

LACP is available only on network node interfaces (NNIs) and enhanced network interfaces (ENIs).

## Syntax Description

*priority* System priority for LACP. The range is 1 to 65535.

## Defaults

The default is 32768.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The **lacp system-priority** command determines which switch in an LACP link controls port priorities. Although this is a global configuration command, the priority only takes effect on EtherChannels that have physical ports that are already configured for LACP.

An LACP channel group can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode. When there are more than eight ports in an LACP channel group, the switch on the controlling end of the link uses port priorities to determine which ports are bundled into the channel and which ports are put in hot-standby mode. Port priorities on the other switch (the noncontrolling end of the link) are ignored.

In priority comparisons, numerically lower values have higher priority. Therefore, the switch with the numerically lower system value (higher priority value) for LACP system priority becomes the controlling switch. If both switches have the same LACP system priority (for example, they are both configured with the default setting of 32768), the LACP system ID (the switch MAC address) determines which switch is in control.

The **lacp system-priority** command applies to all LACP EtherChannels on the switch.

Use the **show etherchannel summary** privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag).

For more information about configuring LACP on physical ports, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

---

**Examples**

This example shows how to set the LACP system priority:

```
Switch(config)# lACP system-priority 20000
```

You can verify your settings by entering the **show lACP sys-id** privileged EXEC command.

---

**Related Commands**

Command	Description
<a href="#">channel-group</a>	Assigns an Ethernet port to an EtherChannel group.
<a href="#">lACP port-priority</a>	Configures the LACP port priority.
<a href="#">show lACP sys-id</a>	Displays the system identifier that is being used by LACP.

# link state group

Use the **link state group** interface configuration command to configure a port as a member of a link-state group. Use the **no** form of this command to remove the port from the link-state group.

**link state group** [*number*] {**upstream** | **downstream**}

**no link state group** [*number*] {**upstream** | **downstream**}

Syntax Description		
	<i>number</i>	(Optional) Specify the link-state group number. The group number can be 1 to 2. The default is 1.
	<b>upstream</b>	Configure a port as an upstream port for a specific link-state group.
	<b>downstream</b>	Configure a port as a downstream port for a specific link-state group.

**Defaults** The default group is group 1.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** Use the **link state group** interface configuration command to configure a port as an upstream or downstream port for a specific link-state group. If the group number is omitted, the default group is assumed.

An interface can be an aggregation of ports (an EtherChannel), a single switch port in access or trunk mode, or a routed port. Each downstream interface can be associated with one or more upstream interfaces. Upstream interfaces can be bundled together, and each downstream interface can be associated with a single group consisting of multiple upstream interfaces, referred to as link-state groups.

The link state of the downstream interfaces are dependent on the link state of the upstream interfaces in the associated link-state group. If all of the upstream interfaces in a link-state group are in a link-down state, the associated downstream interfaces are forced into a link-down state. If any one of the upstream interfaces in the link-state group is in a link-up state, the associated downstream interfaces are allowed to change to, or remain in, a link-up state.

Follow these guidelines to avoid configuration problems:

- An interface that is defined as an upstream interface cannot also be defined as a downstream interface in the same or a different link-state group. The reverse is also true.
- An interface cannot be a member of more than one link-state group.
- You can configure only two link-state groups per switch.



**Examples**

This example shows how to configure the interfaces as **upstream** in group 2:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/11 - 14
Switch(config-if-range)# link state group 2 downstream
Switch(config-if-range)# end
Switch(config-if)# end
```

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

**Related Commands**

Command	Description
<a href="#">link state track</a>	Enables a link-state group.
<a href="#">show link state group</a>	Displays the link-state group information.
<a href="#">show running-config</a>	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: <a href="http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html">http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html</a> Select the <b>Cisco IOS Commands Master List, Release 12.2</b> to navigate to the command.

# link state track

Use the **link state track** user EXEC command to enable a link-state group. Use the **no** form of this command to disable a link-state group.

**link state track** *[number]*

**no link state track** *[number]*

<b>Syntax Description</b>	<i>number</i>	(Optional) Specify the link-state group number. The group number can be 1 to 2. The default is 1.
---------------------------	---------------	---

**Defaults** Link-state tracking is disabled for all groups.

**Command Modes** Global configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

**Usage Guidelines** Use the **link state track** global configuration command to enable a link-state group.

**Examples** This example shows how enable link-state group 2:

```
Switch(config)# link state track 2
```

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">link state group</a>	Configures an interface as a member of a link-state group.
	<a href="#">show link state group</a>	Displays the link-state group information.
	<a href="#">show running-config</a>	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: <a href="http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html">http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html</a> Select the <b>Cisco IOS Commands Master List, Release 12.2</b> to navigate to the command.

## location (global configuration)

Use the **location global configuration** command to configure location information for an endpoint. Use the **no** form of this command to remove the location information.

**location** { **admin-tag** *string* | **civic-location** **identifier** *id* | **elin-location** *string* **identifier** *id* }

**no location** { **admin-tag** *string* | **civic-location** **identifier** *id* | **elin-location** *string* **identifier** *id* }

### Syntax Description

<b>admin-tag</b>	Configure administrative tag or site information.
<b>civic-location</b>	Configure civic location information.
<b>elin-location</b>	Configure emergency location information (ELIN).
<b>identifier</b> <i>id</i>	Specify the ID for the civic location or the elin location. The ID range is 1 to 4095.
	<b>Note</b> The identifier for the civic location in the LLDP-MED TLV is limited to 250 bytes or less. To avoid error messages about available buffer space during switch configuration, be sure that the total length of all civic-location information specified for each civic-location identifier does not exceed 250 bytes.
<i>string</i>	Specify the site or location information in alphanumeric format.

### Defaults

This command has no default setting.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

After entering the **location civic-location identifier** *id* global configuration command, you enter civic location configuration mode. In this mode, you can enter the civic location and the postal location information.

The civic-location identifier must not exceed 250 bytes.

Use the **no lldp med-tlv-select location** information interface configuration command to disable the location TLV. The location TLV is enabled by default. For more information, see the “Configuring LLDP and LLDP-MED” chapter of the software configuration guide for this release.

### Examples

This example shows how to configure civic location information on the switch:

```
Switch(config)# location civic-location identifier 1
Switch(config-civic)# number 3550
Switch(config-civic)# primary-road-name "Cisco Way"
Switch(config-civic)# city "San Jose"
```

## location (global configuration)

```
Switch(config-civic)# state CA
Switch(config-civic)# building 19
Switch(config-civic)# room C6
Switch(config-civic)# county "Santa Clara"
Switch(config-civic)# country US
Switch(config-civic)# end
```

You can verify your settings by entering the **show location civic-location** privileged EXEC command.

This example shows how to configure the emergency location information location on the switch:

```
Switch (config)# location elin-location 14085553881 identifier 1
```

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

### Related Commands

Command	Description
<a href="#">location (interface configuration)</a>	Configures the location information for an interface.
<a href="#">show location</a>	Displays the location information for an endpoint.

# location (interface configuration)

Use the **location interface** command to enter location information for an interface. Use the **no** form of this command to remove the interface location information.

**location** { **additional-location-information** *word* | **civic-location-id** *id* | **elin-location-id** *id* }

**no location** { **additional-location-information** *word* | **civic-location-id** *id* | **elin-location-id** *id* }

Syntax Description	additional-location-information	Configure additional information for a location or place.
	<i>word</i>	Specify a word or phrase that provides additional location information.
	<b>civic-location-id</b>	Configure global civic location information for an interface.
	<b>elin-location-id</b>	Configure emergency location information for an interface.
	<i>id</i>	Specify the ID for the civic location or the elin location. The ID range is 1 to 4095.
	<b>Note</b>	The identifier for the civic location in the LLDP-MED TLV is limited to 250 bytes or less. To avoid error messages about available buffer space during switch configuration, be sure that the total length of all civic-location information specified for each civic-location identifier does not exceed 250 bytes.

**Defaults** This command has no default setting.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** After entering the **location civic-location-id** *id* interface configuration command, you enter civic location configuration mode. In this mode, you can enter the additional location information.

The civic-location identifier must not exceed 250 bytes.

**Examples** These examples show how to enter civic location information for an interface:

```
Switch(config-if)# int g1/0/1
Switch(config-if)# location civic-location-id 1
Switch(config-if)# end
```

```
Switch(config-if)# int g2/0/1
Switch(config-if)# location civic-location-id 1
Switch(config-if)# end
```

## location (interface configuration)

You can verify your settings by entering the **show location civic interface** privileged EXEC command.

This example shows how to enter emergency location information for an interface:

```
Switch(config)# int g2/0/2
Switch(config-if)# location elin-location-id 1
Switch(config-if)# end
```

You can verify your settings by entering the **show location elin interface** privileged EXEC command.

### Related Commands

Command	Description
<a href="#">location (global configuration)</a>	Configures the location information for an endpoint.
<a href="#">show location</a>	Displays the location information for an endpoint.

# logging event

Use the **logging event** interface configuration command to enable notification of interface link status changes. Use the **no** form of this command to disable notification.

**logging event** { **bundle-status** | **link-status** | **spanning-tree** | **status** | **trunk status** }

**no logging event** { **bundle-status** | **link-status** | **spanning-tree** | **status** | **trunk status** }

Syntax Description	Command	Description
	<b>bundle-status</b>	Enable notification of BUNDLE and UNBUNDLE messages.
	<b>link-status</b>	Enable notification of interface data link status changes.
	<b>spanning-tree</b>	Enable notification of spanning-tree events.
	<b>status</b>	Enable notification of spanning-tree state change messages.
	<b>trunk-status</b>	Enable notification of trunk-status messages.

**Defaults** Event logging is disabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Examples** This example shows how to enable spanning-tree logging:

```
Switch(config-if)# logging event spanning-tree
```

# logging file

Use the **logging file** global configuration command to set logging file parameters. Use the **no** form of this command to return to the default setting.

**logging file** *filesystem:filename* [*max-file-size* [*min-file-size*]] [*severity-level-number* | *type*]

**no logging file** *filesystem:filename* [*severity-level-number* | *type*]

## Syntax Description

<i>filesystem:filename</i>	Alias for a flash file system. Contains the path and name of the file that contains the log messages.  The syntax for the local flash file system: <b>flash:</b>
<i>max-file-size</i>	(Optional) Specify the maximum logging file size. The range is 4096 to 2147483647.
<i>min-file-size</i>	(Optional) Specify the minimum logging file size. The range is 1024 to 2147483647.
<i>severity-level-number</i>	(Optional) Specify the logging severity level. The range is 0 to 7. See the <i>type</i> option for the meaning of each level.
<i>type</i>	(Optional) Specify the logging type. These keywords are valid: <ul style="list-style-type: none"> <li>• <b>emergencies</b>—System is unusable (severity 0).</li> <li>• <b>alerts</b>—Immediate action needed (severity 1).</li> <li>• <b>critical</b>—Critical conditions (severity 2).</li> <li>• <b>errors</b>—Error conditions (severity 3).</li> <li>• <b>warnings</b>—Warning conditions (severity 4).</li> <li>• <b>notifications</b>—Normal but significant messages (severity 5).</li> <li>• <b>information</b>—Information messages (severity 6).</li> <li>• <b>debugging</b>—Debugging messages (severity 7).</li> </ul>

## Defaults

The minimum file size is 2048 bytes; the maximum file size is 4096 bytes.

The default severity level is 7 (**debugging** messages and numerically lower levels).

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.



**Usage Guidelines**

The log file is stored in ASCII text format in an internal buffer on the switch. You can access logged system messages by using the switch command-line interface (CLI) or by saving them to a properly configured syslog server. If the switch fails, the log is lost unless you had previously saved it to flash memory by using the **logging file flash:filename** global configuration command.

After saving the log to flash memory by using the **logging file flash:filename** global configuration command, you can use the **more flash:filename** privileged EXEC command to display its contents.

The command rejects the minimum file size if it is greater than the maximum file size minus 1024; the minimum file size then becomes the maximum file size minus 1024.

Specifying a *level* causes messages at that level and numerically lower levels to be displayed.

**Examples**

This example shows how to save informational log messages to a file in flash memory:

```
Switch(config)# logging file flash:logfile informational
```

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

**Related Commands**

Command	Description
<b>show running-config</b>	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: <a href="http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html">http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html</a> Select the <b>Cisco IOS Commands Master List, Release 12.2</b> to navigate to the command.

## mac access-group

Use the **mac access-group** interface configuration command to apply a MAC access control list (ACL) to a Layer 2 interface. Use the **no** form of this command to remove all MAC ACLs or the specified MAC ACL from the interface. You create the MAC ACL by using the **mac access-list extended** global configuration command.

**mac access-group** {*name*} **in**

**no mac access-group** {*name*}

### Syntax Description

<i>name</i>	Specify a named MAC access list.
<b>in</b>	Specify that the ACL is applied in the ingress direction. Outbound ACLs are not supported on Layer 2 interfaces.

### Defaults

No MAC ACL is applied to the interface.

### Command Modes

Interface configuration (Layer 2 interfaces only)

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

You can apply MAC ACLs only to ingress Layer 2 interfaces. You cannot apply MAC ACLs to Layer 3 interfaces.

On Layer 2 interfaces, you can filter IP traffic by using IP access lists and non-IP traffic by using MAC access lists. You can filter both IP and non-IP traffic on the same Layer 2 interface by applying both an IP ACL and a MAC ACL to the interface. You can apply no more than one IP access list and one MAC access list to the same Layer 2 interface.

If a MAC ACL is already configured on a Layer 2 interface and you apply a new MAC ACL to the interface, the new ACL replaces the previously configured one.

If you apply an ACL to a Layer 2 interface on a switch, and the switch has an input Layer 3 ACL or a VLAN map applied to a VLAN that the interface is a member of, the ACL applied to the Layer 2 interface takes precedence.

When an inbound packet is received on an interface with a MAC ACL applied, the switch checks the match conditions in the ACL. If the conditions are matched, the switch forwards or drops the packet, according to the ACL.

If the specified ACL does not exist, the switch forwards all packets.



#### Note

For more information about configuring MAC extended ACLs, see the “Configuring Network Security with ACLs” chapter in the software configuration guide for this release.

**Examples**

This example shows how to apply a MAC extended ACL named *macacl2* to an interface:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mac access-group macacl2 in
```

You can verify your settings by entering the **show mac access-group** privileged EXEC command. You can see configured ACLs on the switch by entering the **show access-lists** privileged EXEC command.

**Related Commands**

Command	Description
<b>show access-lists</b>	Displays the ACLs configured on the switch.
<b>show mac access-group</b>	Displays the MAC ACLs configured on the switch.
<b>show running-config</b>	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: <a href="http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html">http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html</a> Select the <b>Cisco IOS Commands Master List, Release 12.2</b> to navigate to the command.

## mac access-list extended

Use the **mac access-list extended** global configuration command to create an access list based on MAC addresses for non-IP traffic. Using this command puts you in the extended MAC access-list configuration mode. Use the **no** form of this command to return to the default setting.



### Note

You cannot apply named MAC extended ACLs to Layer 3 interfaces.

**mac access-list extended** *name*

**no mac access-list extended** *name*

### Syntax Description

*name* Assign a name to the MAC extended access list.

### Defaults

By default, there are no MAC access lists created.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

MAC named extended lists are used with VLAN maps and class maps.

You can apply named MAC extended ACLs to VLAN maps or to Layer 2 interfaces.

You cannot apply named MAC extended ACLs to Layer 3 interfaces.

Entering the **mac access-list extended** command enables the MAC access-list configuration mode. These configuration commands are available:

- **default**: sets a command to its default.
- **deny**: specifies packets to reject. For more information, see the [deny \(MAC access-list configuration\)](#) MAC access-list configuration command.
- **exit**: exits from MAC access-list configuration mode.
- **no**: negates a command or sets its defaults.
- **permit**: specifies packets to forward. For more information, see the [permit \(MAC access-list configuration\)](#) command.



### Note

For more information about MAC extended access lists, see the software configuration guide for this release.

**Examples**

This example shows how to create a MAC named extended access list named *mac1* and to enter extended MAC access-list configuration mode:

```
Switch(config)# mac access-list extended mac1
Switch(config-ext-macl)#
```

This example shows how to delete MAC named extended access list *mac1*:

```
Switch(config)# no mac access-list extended mac1
```

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

**Related Commands**

Command	Description
<a href="#">deny (MAC access-list configuration)</a>	Configures the MAC ACL (in extended MAC-access list configuration mode).
<a href="#">permit (MAC access-list configuration)</a>	
<a href="#">show access-lists</a>	Displays the access lists configured on the switch.
<a href="#">vlan access-map</a>	Defines a VLAN map and enters access-map configuration mode where you can specify a MAC ACL to match and the action to be taken.

## mac address-table aging-time

Use the **mac address-table aging-time** global configuration command to set the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. Use the **no** form of this command to return to the default setting. The aging time applies to all VLANs or a specified VLAN.

**mac address-table aging-time** {0 | 10-1000000} [vlan *vlan-id*]

**no mac address-table aging-time** {0 | 10-1000000} [vlan *vlan-id*]

Syntax Description	0	This value disables aging. Static address entries are never aged or removed from the table.
	10-1000000	Aging time in seconds. The range is 10 to 1000000 seconds.
	vlan <i>vlan-id</i>	(Optional) Specify the VLAN ID to which to apply the aging time. The range is 1 to 4094.

**Defaults** The default is 300 seconds.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** If hosts do not send continuously, increase the aging time to record the dynamic entries for a longer time. Increasing the time can reduce the possibility of flooding when the hosts send again.  
If you do not specify a specific VLAN, this command sets the aging time for all VLANs.

**Examples** This example shows how to set the aging time to 200 seconds for all VLANs:

```
Switch(config)# mac address-table aging-time 200
```

You can verify your setting by entering the **show mac address-table aging-time** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">show mac address-table aging-time</a>	Displays the MAC address table aging time for all VLANs or the specified VLAN.

# mac address-table learning vlan

Use the **mac address-table learning** global configuration command to enable MAC address learning on a VLAN. This is the default state. 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*

## Syntax Description

<i>vlan-id</i>	Specify a single VLAN ID or a range of VLAN IDs separated by a hyphen or comma. Valid VLAN IDs are 1 to 4094. It cannot be an internal VLAN.
----------------	--

## Defaults

By default, MAC address learning is enabled on all VLANs.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

Customers in a service provider network can tunnel a large number of MAC addresses through the network and fill the available MAC address table space. 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 (for example, **no mac address-table learning vlan 223**) or on a range of VLANs (for example, **mac address-table learning vlan 1-10, 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 used internal VLANs, 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 MAC address learning status of all VLANs or a specified VLAN, enter the **show mac-address-table learning [vlan *vlan-id*]** command.

---

### Examples

This example shows how to disable MAC address learning on VLAN 2003:

```
Switch(config)# no mac address-table learning vlan 2003
```

To display MAC address learning status of all VLANs or a specified VLAN, enter the **show mac address-table learning [vlan *vlan-id*]** command.

---

### Related Commands

Command	Description
<a href="#">show mac address-table learning</a>	Displays the MAC address learning status on all VLANs or on the specified VLAN.



# mac address-table move update

Use the **mac address-table move update** global configuration command to enable the MAC address-table move update feature. Use the **no** form of this command to return to the default setting.

**mac address-table move update {receive | transmit}**

**no mac address-table move update {receive | transmit}**

Syntax Description		
<b>receive</b>	Specify that the switch processes MAC address-table move update messages.	
<b>transmit</b>	Specify that the switch sends MAC address-table move update messages to other switches in the network if the primary link goes down and the standby link comes up.	

**Command Modes** Global configuration.

**Defaults** By default, the MAC address-table move update feature is disabled.

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** The MAC address-table move update feature allows the switch to provide rapid bidirectional convergence if a primary (forwarding) link goes down and the standby link begins forwarding traffic. You can configure the access switch to send the MAC address-table move update messages if the primary link goes down and the standby link comes up. You can configure the uplink switches to receive and process the MAC address-table move update messages.

**Examples** This example shows how to configure an access switch to send MAC address-table move update messages:

```
Switch# configure terminal
Switch(conf)# mac address-table move update transmit
Switch(conf)# end
```

This example shows how to configure an uplink switch to get and process MAC address-table move update messages:

```
Switch# configure terminal
Switch(conf)# mac address-table move update receive
Switch(conf)# end
```

You can verify your settings by entering the **show mac address-table move update** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">clear mac address-table move update</a>	Clears the MAC address-table move update global counters.
	<a href="#">debug matm move update</a>	Debugs the MAC address-table move update message processing.
	<a href="#">show mac address-table move update</a>	Displays the MAC address-table move update information on the switch.

# mac address-table notification

Use the **mac address-table notification** global configuration command to enable the MAC address notification feature on the switch. Use the **no** form of this command to return to the default setting.

```
mac address-table notification { change [history-size value | interval value] | mac-move | threshold [[limit percentage] interval time]
```

```
no mac address-table notification { change [history-size value | interval value] | mac-move | threshold [[limit percentage] interval time]
```

Syntax Description		
<b>change</b>		Enable or disable the MAC notification on the switch.
<b>history-size</b> <i>value</i>		(Optional) Configure the maximum number of entries in the MAC notification history table. The range is 1 to 500 entries. The default is 1.
<b>interval</b> <i>value</i>		(Optional) Set the notification trap interval. The switch sends the notification traps when this amount of time has elapsed. The range is 0 to 2147483647 seconds. The default is 1 second.
<b>mac-move</b>		Enable MAC move notification.
<b>threshold</b>		Enable MAC threshold notification.
<b>limit</b> <i>percentage</i>		(Optional) Enter the MAC utilization threshold percentage. The range is 1 to 100 percent. The default is 50 percent.
<b>interval</b> <i>time</i>		(Optional) Enter the time between MAC threshold notifications. The range is 120 to 1000000 seconds. The default is 120 seconds.

## Defaults

By default, the MAC address notification, MAC move, and MAC threshold monitoring are disabled.

The default MAC change trap interval is 1 second.

The default number of entries in the history table is 1.

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
12.2(44)EY	This command was introduced.

## Usage Guidelines

The MAC address notification change feature sends Simple Network Management Protocol (SNMP) traps to the network management system (NMS) whenever a new MAC address is added or an old address is deleted from the forwarding tables. MAC change notifications are generated only for dynamic and secure MAC addresses and are not generated for self addresses, multicast addresses, or other static addresses.

When you configure the **history-size** option, the existing MAC address history table is deleted, and a new table is created.

You enable the MAC address notification change feature by using the **mac address-table notification change** command. You must also enable MAC address notification traps on an interface by using the **snmp trap mac-notification change** interface configuration command and configure the switch to send MAC address traps to the NMS by using the **snmp-server enable traps mac-notification change** global configuration command.

You can also 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.

### Examples

This example shows how to enable the MAC address-table change notification feature, set the interval time to 60 seconds, and set the history-size to 100 entries:

```
Switch(config)# mac address-table notification change
Switch(config)# mac address-table notification change interval 60
Switch(config)# mac address-table notification change history-size 100
```

You can verify your settings by entering the **show mac address-table notification** privileged EXEC command.

### Related Commands

Command	Description
<b>clear mac address-table notification</b>	Clears the MAC address notification global counters.
<b>show mac address-table notification</b>	Displays the MAC address notification settings on all interfaces or on the specified interface.
<b>snmp-server enable traps</b>	Sends the SNMP MAC notification traps when the <b>mac-notification</b> keyword is appended.
<b>snmp trap mac-notification change</b>	Enables the SNMP MAC notification trap on a specific interface.

# mac address-table static

Use the **mac address-table static** global configuration command to add static addresses to the MAC address table. Use the **no** form of this command to remove static entries from the table.

**mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

**no mac address-table static** *mac-addr* **vlan** *vlan-id* [**interface** *interface-id*]

Syntax Description		
<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.
<b>vlan</b> <i>vlan-id</i>		Specify the VLAN for which the packet with the specified MAC address is received. The range is 1 to 4094.
<b>interface</b> <i>interface-id</i>		Interface to which the received packet is forwarded. Valid interfaces include physical ports and port channels.

**Defaults** No static addresses are configured.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Examples** This example shows how to add the static address c2f3.220a.12f4 to the MAC address table. When a packet is received in VLAN 4 with this MAC address as its destination, the packet is forwarded to the specified interface:

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface
gigabitethernet0/1
```

You can verify your setting by entering the **show mac address-table** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">show mac address-table static</a>	Displays static MAC address table entries only.

## mac address-table static drop

Use the **mac address-table static drop** global configuration command to enable unicast MAC address filtering and to configure the switch to drop traffic with a specific source or destination MAC address. Use the **no** form of this command to return to the default setting.

**mac address-table static** *mac-addr* **vlan** *vlan-id* **drop**

**no mac address-table static** *mac-addr* **vlan** *vlan-id*

### Syntax Description

<i>mac-addr</i>	Unicast source or destination MAC address. Packets with this MAC address are dropped.
<b>vlan</b> <i>vlan-id</i>	Specify the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094.

### Defaults

Unicast MAC address filtering is disabled. The switch does not drop traffic for specific source or destination MAC addresses.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

Follow these guidelines when using this feature:

- Multicast MAC addresses, broadcast MAC addresses, and router MAC addresses are not supported. Packets that are forwarded to the CPU are also not supported.
- If you add a unicast MAC address as a static address and configure unicast MAC address filtering, the switch either adds the MAC address as a static address or drops packets with that MAC address, depending on which command was entered last. The second command that you entered overrides the first command.

For example, if you enter the **mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* global configuration command followed by the **mac address-table static** *mac-addr* **vlan** *vlan-id* **drop** command, the switch drops packets with the specified MAC address as a source or destination.

If you enter the **mac address-table static** *mac-addr* **vlan** *vlan-id* **drop** global configuration command followed by the **mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* command, the switch adds the MAC address as a static address.

---

**Examples**

This example shows how to enable unicast MAC address filtering and to configure the switch to drop packets that have a source or destination address of c2f3.220a.12f4. When a packet is received in VLAN 4 with this MAC address as its source or destination, the packet is dropped:

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop
```

This example shows how to disable unicast MAC address filtering:

```
Switch(config)# no mac address-table static c2f3.220a.12f4 vlan 4
```

You can verify your setting by entering the **show mac address-table static** privileged EXEC command.

---

**Related Commands**

Command	Description
<a href="#">show mac address-table static</a>	Displays only static MAC address table entries.

# macro apply

Use the **macro apply** interface configuration command to apply a macro to an interface or to apply and trace a macro configuration on an interface.

```
macro {apply | trace} macro-name [parameter {value}] [parameter {value}]
      [parameter {value}]
```

## Syntax Description

<b>apply</b>	Apply a macro to the specified interface.
<b>trace</b>	Use the <b>trace</b> keyword to apply a macro to an interface and to debug the macro.
<i>macro-name</i>	Specify the name of the macro.
<b>parameter value</b>	(Optional) Specify unique parameter values that are specific to the interface. You can enter up to three keyword-value pairs. Parameter keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value.

## Defaults

This command has no default setting.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

You can use the **macro trace** *macro-name* interface configuration command to apply and show the macros running on an interface or to debug the macro to find any syntax or configuration errors.

If a command fails because of a syntax error or a configuration error when you apply a macro, the macro continues to apply the remaining commands to the interface.

When creating a macro that requires the assignment of unique values, use the **parameter value** keywords to designate values specific to the interface.

Keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value. Any full match of a keyword, even if it is part of a larger string, is considered a match and is replaced by the corresponding value.

Some macros might contain keywords that require a parameter value. You can use the **macro apply** *macro-name* ? command to display a list of any required values in the macro. If you apply a macro without entering the keyword values, the commands are invalid and are not applied.

When you apply a macro to an interface, the macro name is automatically added to the interface. You can display the applied commands and macro names by using the **show running-configuration interface** *interface-id* user EXEC command.

A macro applied to an interface range behaves the same way as a macro applied to a single interface. When you use an interface range, the macro is applied sequentially to each interface within the range. If a macro command fails on one interface, it is still applied to the remaining interfaces.



You can delete a macro-applied configuration on an interface by entering the **default interface interface-id** interface configuration command.

### Examples

After you have created a macro by using the **macro name** global configuration command, you can apply it to an interface. This example shows how to apply a user-created macro called **duplex** to an interface:

```
Switch(config-if)# macro apply duplex
```

To debug a macro, use the **macro trace** interface configuration command to find any syntax or configuration errors in the macro as it is applied to an interface. This example shows how troubleshoot the user-created macro called **duplex** on an interface:

```
Switch(config-if)# macro trace duplex
Applying command...'duplex auto'
%Error Unknown error.
Applying command...'speed nonegotiate'
```

### Related Commands

Command	Description
<a href="#">macro description</a>	Adds a description about the macros that are applied to an interface.
<a href="#">macro global</a>	Applies a macro on a switch or applies and traces a macro on a switch.
<a href="#">macro global description</a>	Adds a description about the macros that are applied to the switch.
<a href="#">macro name</a>	Creates a macro.
<a href="#">show parser macro</a>	Displays the macro definition for all macros or for the specified macro.

# macro description

Use the **macro description** interface configuration command to enter a description about which macros are applied to an interface. Use the **no** form of this command to remove the description.

**macro description** *text*

**no macro description** *text*

<b>Syntax Description</b>	<b>description</b> <i>text</i> Enter a description about the macros that are applied to the specified interface.
---------------------------	--

<b>Defaults</b>	This command has no default setting.
-----------------	--------------------------------------

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

<b>Usage Guidelines</b>	Use the <b>description</b> keyword to associate comment text, or the macro name, with an interface. When multiple macros are applied on a single interface, the description text will be from the last applied macro.
-------------------------	---

This example shows how to add a description to an interface:

```
Switch(config-if)# macro description duplex settings
```

You can verify your settings by entering the **show parser macro description** privileged EXEC command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">macro apply</a>	Applies a macro on an interface or applies and traces a macro on an interface.
	<a href="#">macro global</a>	Applies a macro on a switch or applies and traces a macro on a switch
	<a href="#">macro global description</a>	Adds a description about the macros that are applied to the switch.
	<a href="#">macro name</a>	Creates a macro.
	<a href="#">show parser macro</a>	Displays the macro definition for all macros or for the specified macro.

# macro global

Use the **macro global** global configuration command to apply a macro to a switch or to apply and trace a macro configuration on a switch.

```
macro global {apply | trace} macro-name [parameter {value}] [parameter {value}]
[parameter {value}]
```

## Syntax Description

<b>apply</b>	Apply a macro to the switch.
<b>trace</b>	Apply a macro to a switch and to debug the macro.
<i>macro-name</i>	Specify the name of the macro.
<b>parameter value</b>	(Optional) Specify unique parameter values that are specific to the switch. You can enter up to three keyword-value pairs. Parameter keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value.

## Defaults

This command has no default setting.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

You can use the **macro trace** *macro-name* global configuration command to apply and to show the macros running on a switch or to debug the macro to find any syntax or configuration errors.

If a command fails because of a syntax error or a configuration error when you apply a macro, the macro continues to apply the remaining commands to the switch.

When creating a macro that requires the assignment of unique values, use the **parameter value** keywords to designate values specific to the switch.

Keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value. Any full match of a keyword, even if it is part of a larger string, is considered a match and is replaced by the corresponding value.

Some macros might contain keywords that require a parameter value. You can use the **macro global apply** *macro-name* ? command to display a list of any required values in the macro. If you apply a macro without entering the keyword values, the commands are invalid and are not applied.

When you apply a macro to a switch, the macro name is automatically added to the switch. You can display the applied commands and macro names by using the **show running-configuration** user EXEC command.

You can delete a global macro-applied configuration on a switch only by entering the **no** version of each command contained in the macro.

**Examples**

After you have created a new macro by using the **macro name** global configuration command, you can apply it to a switch. This example shows how to see the **snmp** macro and how to apply the macro and set the hostname to test-server and set the IP precedence value to 7:

```
Switch# show parser macro name snmp
Macro name : snmp
Macro type : customizable

#enable port security, linkup, and linkdown traps
snmp-server enable traps port-security
snmp-server enable traps linkup
snmp-server enable traps linkdown
#set snmp-server host
snmp-server host ADDRESS
#set SNMP trap notifications precedence
snmp-server ip precedence VALUE

-----
Switch(config)# macro global apply snmp ADDRESS test-server VALUE 7
```

To debug a macro, use the **macro global trace** global configuration command to find any syntax or configuration errors in the macro when it is applied to a switch. In this example, the **ADDRESS** parameter value was not entered, causing the `snmp-server host` command to fail while the remainder of the macro is applied to the switch:

```
Switch(config)# macro global trace snmp VALUE 7
Applying command...'snmp-server enable traps port-security'
Applying command...'snmp-server enable traps linkup'
Applying command...'snmp-server enable traps linkdown'
Applying command...'snmp-server host'
%Error Unknown error.
Applying command...'snmp-server ip precedence 7'
```

**Related Commands**

Command	Description
<a href="#">macro apply</a>	Applies a macro on an interface or applies and traces a macro on an interface.
<a href="#">macro description</a>	Adds a description about the macros that are applied to an interface.
<a href="#">macro global description</a>	Adds a description about the macros that are applied to the switch.
<a href="#">macro name</a>	Creates a macro.
<a href="#">show parser macro</a>	Displays the macro definition for all macros or for the specified macro.

# macro global description

Use the **macro global description** global configuration command to enter a description about the macros that are applied to the switch. Use the **no** form of this command to remove the description.

**macro global description** *text*

**no macro global description** *text*

## Syntax Description

**description** *text* Enter a description about the macros that are applied to the switch.

## Defaults

This command has no default setting.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

Use the **description** keyword to associate comment text, or the macro name, with a switch. When multiple macros are applied on a switch, the description text will be from the last applied macro.

This example shows how to add a description to a switch:

```
Switch(config)# macro global description udlld aggressive mode enabled
```

You can verify your settings by entering the **show parser macro description** privileged EXEC command.

## Related Commands

Command	Description
<a href="#">macro apply</a>	Applies a macro on an interface or applies and traces a macro on an interface.
<a href="#">macro description</a>	Adds a description about the macros that are applied to an interface.
<a href="#">macro global</a>	Applies a macro on a switch or applies and traces a macro on a switch.
<a href="#">macro name</a>	Creates a macro.
<a href="#">show parser macro</a>	Displays the macro definition for all macros or for the specified macro.

## macro name

Use the **macro name** global configuration command to create a configuration macro. Use the **no** form of this command to delete the macro definition.

**macro name** *macro-name*

**no macro name** *macro-name*

### Syntax Description

<i>macro-name</i>	Name of the macro.
-------------------	--------------------

### Defaults

This command has no default setting.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

A macro can contain up to 3000 characters. Enter one macro command per line. Use the @ character to end the macro. Use the # character at the beginning of a line to enter comment text within the macro.

You can define mandatory keywords within a macro by using a help string to specify the keywords. Enter **# macro keywords word** to define the keywords that are available for use with the macro. You can enter up to three help string keywords separated by a space. If you enter more than three macro keywords, only the first three are shown.

Macro names are case sensitive. For example, the commands **macro name Sample-Macro** and **macro name sample-macro** will result in two separate macros.

When creating a macro, do not use the **exit** or **end** commands or change the command mode by using **interface interface-id**. This could cause commands that follow **exit**, **end**, or **interface interface-id** to execute in a different command mode.

The **no** form of this command only deletes the macro definition. It does not affect the configuration of those interfaces on which the macro is already applied. You can delete a macro-applied configuration on an interface by entering the **default interface interface-id** interface configuration command.

Alternatively, you can create an *anti-macro* for an existing macro that contains the **no** form of all the corresponding commands in the original macro. Then apply the anti-macro to the interface.

You can modify a macro by creating a new macro with the same name as the existing macro. The newly created macro overwrites the existing macro but does not affect the configuration of those interfaces on which the original macro was applied.

**Examples**

This example shows how to create a macro that defines the duplex mode and speed:

```
Switch(config)# macro name duplex
Enter macro commands one per line. End with the character '@'.
duplex full
speed auto
@
```

This example shows how create a macro with **# macro keywords**:

```
Switch(config)# macro name test
switchport access vlan $VLANID
switchport port-security maximum $MAX
#macro keywords $VLANID $MAX
@
```

This example shows how to display the mandatory keyword values before you apply the macro to an interface:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# macro apply test ?
WORD keyword to replace with a value e.g $VLANID,$MAX
<cr>
```

```
Switch(config-if)# macro apply test $VLANID ?
WORD Value of first keyword to replace
```

```
Switch(config-if)# macro apply test $VLANID 2
WORD keyword to replace with a value e.g $VLANID,$MAX
<cr>
```

```
Switch(config-if)# macro apply test $VLANID 2 $MAX ?
WORD Value of second keyword to replace
```

**Related Commands**

Command	Description
<a href="#">macro apply</a>	Applies a macro on an interface or applies and traces a macro on an interface.
<a href="#">macro description</a>	Adds a description about the macros that are applied to an interface.
<a href="#">macro global</a>	Applies a macro on a switch or applies and traces a macro on a switch
<a href="#">macro global description</a>	Adds a description about the macros that are applied to the switch.
<a href="#">show parser macro</a>	Displays the macro definition for all macros or for the specified macro.

## match (access-map configuration)

Use the **match** access-map configuration command to set the VLAN map to match packets against one or more access lists. Use the **no** form of this command to remove the match parameters.

```
match {ip address {name | number} [name | number] [name | number]...} | {mac address {name} [name] [name]...}
```

```
no match {ip address {name | number} [name | number] [name | number]...} | {mac address {name} [name] [name]...}
```

### Syntax Description

<b>ip address</b>	Set the access map to match packets against an IP address access list.
<b>mac address</b>	Set 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.

### Defaults

The default action is to have no match parameters applied to a VLAN map.

### Command Modes

Access-map configuration

### Command History

Release	Modification
12.2(44)EY	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, and all other packets are matched against MAC access lists.

Both IP and MAC addresses can be specified for the same map entry.

### Examples

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 *a12*.

```
Switch(config)# vlan access-map vmap4
Switch(config-access-map)# match ip address a12
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# vlan filter vmap4 vlan-list 5-6
```



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

Related Commands	Command	Description
	<b>access-list</b>	Configures a standard numbered ACL. For syntax information, select <b>Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 &gt; IP Services Commands</b> .
	<b>action</b>	Specifies the action to be taken if the packet matches an entry in an access control list (ACL).
	<b>ip access list</b>	Creates a named access list. For syntax information, select <b>Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 &gt; IP Services Commands</b> .
	<b>mac access-list extended</b>	Creates a named MAC address access list.
	<b>show vlan access-map</b>	Displays the VLAN access maps created on the switch.
	<b>vlan access-map</b>	Creates a VLAN access map.

## match access-group

Use the **match access-group** class-map configuration command to configure the match criteria for a class map on the basis of the specified access control list (ACL). Use the **no** form of this command to remove the ACL match criteria.

**match access-group** *acl-index-or-name*

**no match access-group** *acl-index-or-name*

### Syntax Description

<i>acl-index-or-name</i>	Number or name of an IP standard or extended access control list (ACL) or MAC ACL. For an IP standard ACL, the ACL index range is 1 to 99 and 1300 to 1999. For an IP extended ACL, the ACL index range is 100 to 199 and 2000 to 2699.
--------------------------	---

### Defaults

No match criteria are defined.

### Command Modes

Class-map configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

The **match access-group** command specifies a numbered or named ACL to use as the match criteria to determine if packets belong to the class specified by the class map.

Before using the **match access-group** command, you must enter the **class-map** global configuration command to specify the name of the class whose match criteria you want to establish.

You can use the **match access-group** classification only on input policy maps.

### Examples

This example shows how to create a class map called *inclass*, which uses the access control list *acl1* as the match criterion:

```
Switch(config)# class-map match-any inclass
Switch(config-cmap)# match access-group acl1
Switch(config-cmap)# exit
```

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

### Related Commands

Command	Description
<a href="#">class-map</a>	Creates a class map to be used for matching packets to the class whose name you specify.
<a href="#">show class-map</a>	Displays quality of service (QoS) class maps.

# match cos

Use the **match cos** class-map configuration command to match a packet based on a Layer 2 class of service (CoS) marking. Use the **no** form of this command to remove the CoS match criteria.

**match cos** [**inner**] *cos-list*

**no match cos inner** *cos-list*

Syntax Description	inner	(Optional) Match a packet based on the C-CoS, the inner (customer) CoS value of an 802.1Q tunnel. If you do not enter the <b>inner</b> keyword, the packet is matched based on service-provider CoS value (S-CoS).
	<i>cos-list</i>	List of up to four CoS values to match against incoming packets. Separate each value with a space. The range is 0 to 7.

**Defaults** No match criteria are defined.

**Command Modes** Class-map configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.
	12.2(53)SE	The <b>inner</b> keyword was added.

**Usage Guidelines** The **match cos** command specifies a CoS value to use as the match criteria to determine if packets belong to the class specified by the class map.

Before using the **match cos** command, you must enter the **class-map** global configuration command to specify the name of the class whose match criteria you want to establish.

- Enter **cos** *cos-list* to match a packet based on the service-provider CoS value (S-CoS). For QinQ, where an incoming packet is tunneled into an S-tag, this is the CoS value in the imposed S-tag. For all other cases, this is the CoS value in the incoming packet.
- Enter **cos inner** *cos-list* to match a packet based on the C-CoS, the inner (customer) CoS value of an 802.1Q tunnel. For QinQ, where an incoming packet is tunneled into an S-tag, this is the CoS value in the incoming customer packet. For all other cases, this command has no effect.

You can *specify* up to four Layer 2 CoS values to match against the packet. Separate each value with a space. The range is 0 to 7.

Matching of CoS values is supported only on ports carrying Layer 2 VLAN-tagged traffic. That is, you can use the **cos** classification only on IEEE 802.1Q trunk ports.

You can use **match cos** classification in input and output policy maps.

**Examples**

This example shows how to create a class map called *inclass*, which matches all the incoming traffic with service provider CoS values of 1 and 4:

```
Switch(config)# class-map match-any in-class
Switch(config-cmap)# match cos 1 4
Switch(config-cmap)# exit
```

This example shows how to create a class map called *video-L2*, which matches all the incoming traffic with customer CoS value of 3:

```
Switch(config)# class-map match-any video-L2
Switch(config-cmap)# match cos inner 3
Switch(config-cmap)# exit
```

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

**Related Commands**

Command	Description
<a href="#">class-map</a>	Creates a class map to be used for matching packets to the class whose name you specify.
<a href="#">show class-map</a>	Displays quality of service (QoS) class maps.

# match dot1ad dei

Use the **match dot1ad dei** class-map configuration command to match a packet based on the drop eligibility indicator (DEI) in an IEEE 802.1ad frame. Use the **no** form of this command to remove the DEI match criteria.

```
match dot1ad dei dei_value
```

```
no match dot1ad dei
```

<b>Syntax Description</b>	<i>dei-value</i>	Match a packet based on the DEI bit in the 802.1ad packet. The range is 0 to 1.
---------------------------	------------------	---

<b>Defaults</b>	No match criteria are defined.
-----------------	--------------------------------

<b>Command Modes</b>	Class-map configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(55)SE	The <b>inner</b> keyword was added.

<b>Usage Guidelines</b>	<p>The <b>match dot1ad dei</b> command specifies using the DEI bit of the incoming packet as the match criteria to determine if packets belong to the class specified by the class map.</p> <p>You can use the command with <b>match-any</b> or <b>match-all</b> options.</p> <p>You can use this match criteria for per-port and per-port, per-VLAN policies within a child policy map. Matching on the DEI bit is supported for both ingress and egress classification, but only 802.1ad S-NNI ports can match on the DEI bit.</p> <p>You can verify your settings by entering the <b>show class-map</b> privileged EXEC command.</p>
-------------------------	---

<b>Examples</b>	<p>This example shows how to create a class map called <i>class1</i>, which matches traffic on the DEI bit and the CoS value:</p>
-----------------	---

```
Switch(config)# class-map match-any class1
Switch(config-cmap)# match dot1ad dei 0
Switch(config-cmap)# match cos 0
Switch(config-cmap)# exit
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>class-map</b>	Creates a class map to be used for matching packets to the class whose name you specify.
	<b>ethernet dot1ad</b>	Configures an interface as an 802.1ad C-port or S-port.

■ match dot1ad dei

Command	Description
set dot1ad dei	Defines a policy map set criteria as using the DEI bit.
<a href="#">show class-map</a>	Displays quality of service (QoS) class maps.

# match ip dscp

Use the **match ip dscp** class-map configuration command to identify a specific IPv4 Differentiated Service Code Point (DSCP) value as match criteria for a class. Use the **no** form of this command to remove the match criteria.

**match ip dscp** *dscp-list*

**no match ip dscp** *dscp-list*

## Syntax Description

*ip-dscp-list*

List of up to eight IPv4 DSCP values to match against incoming packets. Separate each value with a space. The range is 0 to 63. You can also enter a mnemonic name for a commonly used value.

See the “Configuring QoS” chapter in the software configuration guide for this release for information about other options for specifying DSCP values.

## Defaults

No match criteria are defined.

## Command Modes

Class-map configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The **match ip dscp** command specifies a DSCP value to use as the match criteria to determine if packets belong to the class specified by the class map.

This command is used by the class map to identify a specific DSCP value marking on a packet. In this context, DSCP values are used as markings only and have no mathematical significance. For example, the DSCP value of 2 is not greater than 1, but merely indicates that a packet marked with a value of 2 is different than one marked with a value of 1. You define the treatment of these marked packets by setting QoS policies in policy-map class configuration mode.

Before using the **match ip dscp** command, you must enter the **class-map** global configuration command to specify the name of the class whose match criteria you want to establish.

You can enter up to eight DSCP values in one match statement. For example, if you wanted the DSCP values of 0, 1, 2, 3, 4, 5, 6, or 7, enter the **match ip dscp 0 1 2 3 4 5 6 7** command. The packet must match only one (not all) of the specified IPv4 DSCP values to belong to the class.

You can use **match ip dscp** classification in input and output policy maps.

**Examples**

This example shows how to create a class map called *inclass*, which matches all the incoming traffic with DSCP values of 10, 11, and 12:

```
Switch(config)# class-map match-any in-class
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# exit
```

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

**Related Commands**

Command	Description
<a href="#">class-map</a>	Creates a class map to be used for matching packets to the class whose name you specify.
<a href="#">show class-map</a>	Displays quality of service (QoS) class maps.



# match ip precedence

Use the **match ip precedence** class-map configuration command to identify IPv4 precedence values as match criteria for a class. Use the **no** form of this command to remove the match criteria.

**match ip precedence** *ip-precedence-list*

**no match ip precedence** *ip-precedence-list*

Syntax Description	ip precedence	List of up to four IPv4 precedence values to match against incoming packets.
	<i>ip-precedence-list</i>	Separate each value with a space. The range is 0 to 7.

**Defaults** No match criteria are defined.

**Command Modes** Class-map configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** The **match ip precedence** command specifies an IPv4 precedence value to use as the match criteria to determine if packets belong to the class specified by the class map.

The precedence values are used as marking only. In this context, the IP precedence values have no mathematical significance. For example, the precedence value of 2 is not greater than 1, but merely indicates that a packet marked with a value of 2 is different than one marked with a value of 1. You define the treatment of these marked packets by setting QoS policies in policy-map class configuration mode.

Before using the **match ip precedence** command, you must enter the **class-map** global configuration command to specify the name of the class whose match criteria you want to establish.

You can enter up to four IPv4 precedence values in one match statement. For example, if you wanted the IP precedence values of 0, 1, 2, or 7, enter the **match ip precedence 0 1 2 7** command. The packet must match only one (not all) of the specified IP precedence values to belong to the class.

You can use **match ip precedence** classification in input and output policy maps.

**Examples** This example shows how to create a class map called *class*, which matches all the incoming traffic with IP-precedence values of 5, 6, and 7:

```
Switch(config)# class-map match-any in-class
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# exit
```

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

■ match ip precedence

Related Commands	Command	Description
	<a href="#">class-map</a>	Creates a class map to be used for matching packets to the class whose name you specify.
	<a href="#">show class-map</a>	Displays quality of service (QoS) class maps.

# match qos-group

Use the **match qos-group** class-map configuration command to identify a specific quality of service (QoS) group value as a match criterion for a class. Use the **no** form of this command to remove the match criterion.

**match qos-group** *value*

**no match qos-group** *value*

<b>Syntax Description</b>	<b>qos-group</b> <i>value</i>	A quality of service group value. The range is from 0 to 99.
<b>Defaults</b>	No match criterion are defined.	
<b>Command Modes</b>	Class-map configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

**Usage Guidelines**

The **match qos-group** command specifies a QoS group value to use as the match criterion to determine if packets belong to the class specified by the class map.

The QoS-group values are used as marking only and have no mathematical significance. For example, the precedence value of 2 is not greater than 1, but merely indicates that a packet marked with a value of 2 is different than one marked with a value of 1. You define the treatment of these marked packets by setting QoS policies in policy-map class configuration mode.

The QoS-group value is local to the switch, meaning that the QoS-group value marked on a packet does not leave the switch when the packet leaves the switch. If you require a marking that remains with the packet, use IP Differentiated Service Code Point (DSCP) values, IP precedence values, or another method of packet marking.

Before using the **match qos-group** command, you must enter the **class-map** global configuration command to specify the name of the class whose match criteria you want to establish.

You can use the **match qos-group** classification only on output policy maps.

There can be no more than 100 QoS groups on the switch (0 to 99).

**Examples** This example shows how to classify traffic by using QoS group 13 as the match criterion:

```
Switch(config)# class-map match-any inclass
Switch(config-cmap)# match qos-group 13
Switch(config-cmap)# exit
```

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

■ match qos-group

Related Commands	Command	Description
	<a href="#">class-map</a>	Creates a class map to be used for matching packets to the class whose name you specify.
	<a href="#">show class-map</a>	Displays QoS class maps.

# match vlan

Use the **match vlan** class-map configuration command in the parent policy of a hierarchical policy map to apply QoS policies to frames carried on a user-specified VLAN for a given interface. You can use hierarchical policy maps for per-VLAN classification on trunk ports. Use the **no** form of this command to remove the match criteria.

**match vlan** [**inner**] *vlan-list*

**no match vlan** [**inner**] *vlan-list*

Syntax Description	inner	(Optional) Match a packet based on the C-VLAN, the inner customer VLAN ID of an 802.1Q tunnel. If you do not enter the <b>inner</b> keyword, the packet is matched based on the service-provider VLAN ID (S-VLAN).
	<i>vlan-list</i>	Specify a VLAN ID or a range of VLANs to match against incoming packets in a parent policy map for per-port, per-VLAN QoS on a trunk port. You can enter up to 30 VLAN IDs. Use a hyphen for a range of VLANs. A VLAN range is counted as two VLAN IDs. Use a space to separate individual VLANs. The range is 1 to 4094.

**Defaults** No match criteria are defined.

**Command Modes** Class-map configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.
	12.2(53)SE	This <b>inner</b> keyword was added.

**Usage Guidelines** The feature is supported only using a 2-level hierarchical input policy map, where the parent-level defines the VLAN-based classification, and the child-level defines the QoS policy to be applied to the corresponding VLAN(s).

You can configure multiple service classes at the parent-level to match different combinations of VLANs, and you can apply independent QoS policies to each parent-service class using any child-policy map.

A policy is considered a parent policy map when it has one or more of its classes associated with a child policy-map. Each class within a parent policy map is called a parent class. You can configure only the **match vlan** command in parent classes. You cannot configure the **match vlan** command in classes within the child policy map.

- Enter **vlan** *vlan-id* to match a packet based on the service-provider VLAN ID (S-VLAN). For QinQ, where an incoming customer packet is tunneled into an S-tag, this is the VLAN value in the imposed S-tag. For all other cases, this is the VLAN value in the incoming packet.

- Enter **vlan inner** *vlan-id* to match a packet based on the C-VLAN, the inner customer VLAN ID of an 802.1Q tunnel. For QinQ, where an incoming customer packet is tunneled into an S-tag, this is the VLAN value in the incoming customer packet. For all other cases, this command has no effect.

A per-port, per-VLAN parent-level class map supports only a child-policy association; it does not allow any actions to be configured. In addition, for a parent-level class map, you cannot configure an action or a child-policy association for the class **class-default**.

You cannot configure a mixture of Layer 2 and Layer 3 class maps in a child policy map. When you attempt to associate such a child policy map with a parent policy, the configuration is rejected. However, you can associate Layer 2 child policies and Layer 3 child policies with different parent-level class maps.

Per-port, per-VLAN QoS is supported only on IEEE 802.1Q trunk ports.

Once a per-port, per-vlan hierarchical policy-map is attached to an interface, a parent-class with vlan-based classification can not be dynamically added or removed. The service policy needs to be detached from the interface before making this configuration change.

When the child policy map attached to a VLAN or set of VLANs contains only Layer 3 classification (**match ip dscp**, **match ip precedence**, **match IP ACL**), you must be careful to ensure that these VLANs are not carried on any port other than the one on which this per-port, per-VLAN policy is attached. Not following this restriction could result in improper QoS behavior for traffic ingressing the switch on these VLANs.

We also recommend that you restrict VLAN membership on the trunk ports to which the per-port, per-VLAN is applied by using the **switchport trunk allowed vlan** interface configuration command. Overlapping VLAN membership between trunk ports that have per-port, per-VLAN policies with Layer 3 classification could also result in unexpected QoS behavior.

Before using the **match vlan** command, you must enter the **class-map** global configuration command to specify the name of the class whose match criteria you want to establish.

## Examples

In this example, the class maps in the child-level policy map specify matching criteria for voice and video traffic, and the child policy map sets the action for input policing each type of traffic. The parent-level policy map specifies the VLANs to which the child policy maps are applied on the specified port.

```
Switch(config)# class-map match-any dscp-23 video
Switch(config-cmap)# match ip dscp 23
Switch(config-cmap)# exit
Switch(config)# class-map match-any dscp-63 voice
Switch(config-cmap)# match ip dscp-63
Switch(config-cmap)# exit
Switch(config)# class-map match-any customer-1-vlan
Switch(config-cmap)# match vlan 100
Switch(config-cmap)# match vlan 200
Switch(config-cmap)# match vlan 300
Switch(config-cmap)# exit
```



### Note

You can also enter the match criteria as **match vlan 100 200 300** with the same result.

```
Switch(config)# policy-map child policy-1
Switch(config-pmap)# class dscp-63 voice
Switch(config-pmap-c)# police cir 10000000 bc 50000
Switch(config-pmap-c)# conform-action set-cos-transmit 5
Switch(config-pmap-c)# exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# class dscp-23 video
Switch(config-pmap-c)# set cos 4
```

```
Switch(config-pmap-c) # set ip precedence 4
Switch(config-pmap-c) # exit

Switch(config) # policy-map parent-customer-1
Switch(config-pmap) # class customer-1-vlan
Switch(config-pmap-c) # service-policy ingress-policy-1
Switch(config-pmap-c) # exit
```

In this example, all packets with an S-VLAN of 100 *and* a C-VLAN of 200 (packets with C-VLAN 200 tunneled into S-VLAN 100) are classified by the class *L2-vpn* and packets with an S-VLAN of 110 *and* a C-VLAN in the range of 210 to 220 (packets with C-VLANs 210 to 220 tunneled into S-VLAN 110) are classified by the class *voice-gateway*.

```
Switch(config) # class-map match-all L2-vpn
Switch(config-cmap) # match vlan 100
Switch(config-cmap) # match vlan inner 200
Switch(config-cmap) # exit

Switch(config) # class-map match-all voice-gateway
Switch(config-cmap) # match vlan 110
Switch(config-cmap) # match vlan inner 210-220
Switch(config-cmap) # exit
```

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

#### Related Commands

Command	Description
<a href="#">class-map</a>	Creates a class map to be used for matching packets to a specified class name.
<a href="#">show class-map</a>	Displays quality of service (QoS) class maps.

## mdix auto

Use the **mdix auto** interface configuration command to enable the automatic medium-dependent interface crossover (auto-MDIX) feature on the interface. When auto-MDIX is enabled, the interface automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately. Use the **no** form of this command to disable auto-MDIX.

**mdix auto**

**no mdix auto**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Auto-MDIX is enabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** When you enable auto-MDIX on an interface, you must also set the speed and duplex on the interface to **auto** so that the feature operates correctly. If the port is a user network interface (UNI) or enhanced network interfaces (ENI), you must use the **no shutdown** interface configuration command to enable it before using the **mdix auto** command. UNIs and ENIs are disabled by default. Network node interfaces (NNIs) are enabled by default.

When auto-MDIX (along with autonegotiation of speed and duplex) is enabled on one or both of connected interfaces, link up occurs, even if the required cable type (straight-through or crossover) is not present.

Auto-MDIX is supported on all 10/100-Mbps interfaces and on 10/100/1000BASE-T/BASE-TX small form-factor pluggable (SFP)-module interfaces. It is not supported on 1000BASE-SX or -LX SFP module interfaces.

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

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

You can verify the operational state of auto-MDIX on the interface by entering the **show controllers ethernet-controller interface-id phy** privileged EXEC command.



Related Commands	Command	Description
	<code>show controllers ethernet-controller interface-id phy</code>	Displays general information about internal registers of an interface, including the operational state of auto-MDIX.

# media-type

Use the **media-type** interface configuration command to manually select the interface and type of a dual-purpose port or to enable the switch to dynamically select the type that first links up. Use the **no** form of this command to return to the default setting.

**media-type** { **auto-select** | **rj45** | **sfp** }

**no media-type**

## Syntax Description

<b>auto-select</b>	Enable the switch to dynamically select the type based on the first to link up.
<b>rj45</b>	Select the RJ-45 interface.
<b>sfp</b>	Select the small form-factor pluggable (SFP) module interface.

## Defaults

The default is that the switch dynamically selects the link (**auto-select**)

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

You cannot use the RJ-45 interface and the SFP interface of the dual-purpose ports simultaneously to provide redundant links.

When you select **auto-select**, the switch dynamically selects the type that first links up. This is the default mode. The switch disables the other media type until the active link goes down. When the active link goes down, the switch enables both types until one of them links up. If there are active links on both media, the SFP link has priority. In auto-select mode, the switch configures both types with autonegotiation of speed and duplex (the default).

When you select **rj45**, the switch disables the SFP module interface. If you connect a cable to the SFP port, it cannot attain a linkup even if the RJ-45 side is down or is not connected. In this mode, the dual-purpose port behaves like a 10/100/1000BASE-TX interface. You can configure the speed and duplex settings consistent with this interface type.

When you select **sfp**, the switch disables the RJ-45 interface. If you connect a cable to this port, it cannot attain a linkup even if the SFP module side is down or if the SFP module is not present. Based on the type of installed SFP module, you can configure the speed and duplex settings consistent with this interface type.

To configure speed or duplex settings on a dual-purpose port, you must first select the media type. If you configure **auto-select**, you cannot configure the **speed** and **duplex** interface configuration commands. When you change the interface type, the speed and duplex configurations are removed. The switch configures both types to autonegotiate speed and duplex (the default).

When the media type is **auto-select**, the switch uses these criteria to select the media type:




---

**Note** An SFP is not *installed* until it has a fiber or copper cable plugged into the SFP module.

---

- If only one media type is installed, that interface is active and remains active until the media is removed or the switch is reloaded.
- If you install both media types in a dual-purpose port that is enabled, the switch selects the active link based on which type is installed first.
- When the switch powers on with both cables connected, or when you enable a dual-purpose port through the **shutdown** and the **no shutdown** interface configuration commands, the switch gives preference to the SFP module interface. In all other situations, the switch selects the active link based on the type that first links up.

---

### Examples

This example shows how to select the SFP interface:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# media-type sfp
```

You can verify your setting by entering the **show interfaces *interface-id* capabilities** or the **show interfaces *interface-id* transceiver properties** privileged EXEC commands.

---

### Related Commands

Command	Description
<b>show interfaces capabilities</b>	Displays the capabilities of all interfaces or the specified interface.
<b>show interfaces transceiver properties</b>	Displays speed, duplex, and media-type settings on all interfaces or the specified interface.

## monitor session

Use the **monitor session** global configuration command to start a new Switched Port Analyzer (SPAN) session or Remote SPAN (RSPAN) source or destination session, to enable incoming traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance), to add or delete interfaces or VLANs to or from an existing SPAN or RSPAN session, and to limit (filter) SPAN source traffic to specific VLANs. Use the **no** form of this command to remove the SPAN or RSPAN session or to remove source or destination interfaces or filters from the SPAN or RSPAN session. For destination interfaces, the **encapsulation dot1q** or **encapsulation replicate** keywords are ignored with the **no** form of the command.

**monitor session** *session\_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation** {**dot1q** | **replicate**}] [**ingress** {[**dot1q** | **untagged**] **vlan** *vlan-id*]} | {**remote vlan** *vlan-id*}

**monitor session** *session\_number* **filter vlan** *vlan-id* [, | -]

**monitor session** *session\_number* **source** {**interface** *interface-id* [, | -] [**both** | **rx** | **tx**]} | {**vlan** *vlan-id* [, | -] [**both** | **rx** | **tx**]} | {**remote vlan** *vlan-id*}

**no monitor session** {*session\_number* | **all** | **local** | **remote**}

**no monitor session** *session\_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation** {**dot1q** | **replicate**}] [**ingress** {[**dot1q** | **untagged**] **vlan** *vlan-id*]} | {**remote vlan** *vlan-id*}

**no monitor session** *session\_number* **filter vlan** *vlan-id* [, | -]

**no monitor session** *session\_number* **source** {**interface** *interface-id* [, | -] [**both** | **rx** | **tx**]} | {**vlan** *vlan-id* [, | -] [**both** | **rx** | **tx**]} | {**remote vlan** *vlan-id*}

### Syntax Description

<i>session_number</i>	Specify the session number identified with the SPAN or RSPAN session. The range is 1 to 66.
<b>interface</b> <i>interface-id</i>	Specify the destination or source interface for a SPAN or RSPAN session. Valid interfaces are physical ports (including type and port number). For <b>source interface</b> , <b>port channel</b> is also a valid interface type, and the valid range is 1 to 48.
<b>destination</b>	Specify the SPAN or RSPAN destination. A destination must be a physical port.
<b>encapsulation replicate</b>	(Optional) Specify the encapsulation method. If not selected, the default is to send packets in native form (untagged). <ul style="list-style-type: none"> <li><b>dot1q</b>—Specify IEEE 802.1Q encapsulation.</li> <li><b>replicate</b>—Specify that the destination interface replicates the source interface encapsulation method.</li> </ul> <p><b>Note</b> Entering these keywords is valid only for local SPAN. For RSPAN, the RSPAN VLAN ID overwrites the original VLAN ID; therefore packets are always sent untagged.</p>
<b>ingress</b>	(Optional) Enable ingress traffic forwarding.
<b>dot1q vlan</b> <i>vlan-id</i>	Specify ingress forwarding using IEEE 802.1Q encapsulation with the specified VLAN as the default VLAN for ingress traffic.

<b>untagged vlan</b> <i>vlan-id</i>	Specify ingress forwarding using untagged encapsulation with the specified VLAN as the default VLAN for ingress traffic
<b>vlan</b> <i>vlan-id</i>	When used with only the <b>ingress</b> keyword, set default VLAN for ingress traffic.
<b>remote vlan</b> <i>vlan-id</i>	Specify the remote VLAN for an RSPAN source or destination session. The range is 2 to 1001 and 1006 to 4094.  <b>Note</b> The RSPAN VLAN cannot be VLAN 1 (the default VLAN) or VLAN IDs 1002 to 1005 (reserved for Token Ring and FDDI VLANs).
,	(Optional) Specify a series of interfaces or VLANs, or separate a range of interfaces or VLANs from a previous range. Enter a space before and after the comma.
-	(Optional) Specify a range of interfaces or VLANs. Enter a space before and after the hyphen.
<b>filter vlan</b> <i>vlan-id</i>	Specify 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.
<b>source</b>	Specify the SPAN or RSPAN source. A source can be a physical port, a port channel, or a VLAN.
<b>both, rx, tx</b>	(Optional) Specify the traffic direction to monitor. If you do not specify a traffic direction, the source interface sends both transmitted and received traffic.
<b>source vlan</b> <i>vlan-id</i>	Specify the SPAN source interface as a VLAN ID. The range is 1 to 4094.
<b>all, local, remote</b>	Specify <b>all</b> , <b>local</b> , or <b>remote</b> with the <b>no monitor session</b> command to clear all SPAN and RSPAN, all local SPAN, or all RSPAN sessions.

**Defaults**

No monitor sessions are configured.

On a source interface, the default is to monitor both received and transmitted traffic.

On a trunk interface used as a source port, all VLANs are monitored.

If **encapsulation dot1q** or **encapsulation replicate** is not specified on a local SPAN destination port, packets are sent in native form with no encapsulation tag.

Ingress forwarding is disabled on destination ports.

**Command Modes**

Global configuration

**Command History**

Release	Modification
12.2(44)EY	This command was introduced.

**Usage Guidelines**

Traffic that enters or leaves source ports or source VLANs can be monitored by using SPAN or RSPAN. Traffic routed to source ports or source VLANs cannot be monitored.

You can set a combined maximum of two local SPAN sessions and RSPAN source sessions. You can have a total of 66 SPAN and RSPAN sessions on a switch.

You can have a maximum of 64 destination ports on a switch.

Each session can include multiple ingress or egress source ports or VLANs, but you cannot combine source ports and source VLANs in a single session. Each session can include multiple destination ports.

When you use VLAN-based SPAN (VSPAN) to analyze network traffic in a VLAN or set of VLANs, all active ports in the source VLANs become source ports for the SPAN or RSPAN session. Trunk ports are included as source ports for VSPAN, and only packets with the monitored VLAN ID are sent to the destination port.

You can monitor traffic on a single port or VLAN or on a series or range of ports or VLANs. You select a series or range of interfaces or VLANs by using the [, | -] options.

If you specify a series of VLANs or interfaces, you must enter a space before and after the comma. If you specify a range of VLANs or interfaces, you must enter a space before and after the hyphen (-).

EtherChannel ports cannot be configured as SPAN or RSPAN destination ports. A physical port that is a member of an EtherChannel group can be used as a destination port, but it cannot participate in the EtherChannel group while it is as a SPAN destination.

A private-VLAN port cannot be configured as a SPAN destination port.

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 on a port that is a SPAN or RSPAN destination port; however, IEEE 802.1x is disabled until the port is removed as a SPAN destination. (If IEEE 802.1x is not available on the port, the switch returns an error message.) You can enable IEEE 802.1x on a SPAN or RSPAN source port.

VLAN filtering refers to analyzing network traffic on a selected set of VLANs on trunk source ports. By default, all VLANs are monitored on trunk source ports. You can use the **monitor session session\_number filter vlan vlan-id** command to limit SPAN traffic on trunk source ports to only the specified VLANs.

VLAN monitoring and VLAN filtering are mutually exclusive. If a VLAN is a source, VLAN filtering cannot be enabled. If VLAN filtering is configured, a VLAN cannot become a source.

If ingress traffic forwarding is enabled for a network security device, the destination port forwards traffic at Layer 2.

Destination ports can be configured to act in these ways:

- When you enter **monitor session session\_number destination interface interface-id** with no other keywords, egress encapsulation is untagged, and ingress forwarding is not enabled.
- When you enter **monitor session session\_number destination interface interface-id 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.)
- 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**.

**Examples**

This example shows how to create a local SPAN session 1 to monitor both sent and received traffic on source port 1 to destination port 2:

```
Switch(config)# monitor session 1 source interface gigabitethernet0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet0/2
```

This example shows how to delete a destination port from an existing local SPAN session:

```
Switch(config)# no monitor session 2 destination gigabitethernet0/2
```

This example shows how to limit SPAN traffic in an existing session only to specific VLANs:

```
Switch(config)# monitor session 1 filter vlan 100 - 110
```

This example shows how to configure RSPAN source session 1 to monitor multiple source interfaces and to configure the destination RSPAN VLAN 900.

```
Switch(config)# monitor session 1 source interface gigabitethernet0/1
Switch(config)# monitor session 1 source interface port-channel 2 tx
Switch(config)# monitor session 1 destination remote vlan 900
Switch(config)# end
```

This example shows how to configure an RSPAN destination session 10 in the switch receiving the monitored traffic.

```
Switch(config)# monitor session 10 source remote vlan 900
Switch(config)# monitor session 10 destination interface gigabitethernet0/2
```

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that supports IEEE 802.1Q encapsulation. Egress traffic replicates the source; ingress traffic uses IEEE 802.1Q encapsulation.

```
Switch(config)# monitor session 2 destination interface gigabitethernet0/2 encapsulation
replicate ingress dot1q vlan 5
```

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that does not support encapsulation. Egress traffic and ingress traffic are untagged.

```
Switch(config)# monitor session 2 destination interface gigabitethernet0/2 ingress
untagged vlan 5
```

You can verify your settings by entering the **show monitor** privileged EXEC command. You can display SPAN and RSPAN configuration on the switch by entering the **show running-config** privileged EXEC command. SPAN information appears near the end of the output.

**Related Commands**

Command	Description
<a href="#">remote-span</a>	Configures an RSPAN VLAN in vlan configuration mode.
<a href="#">show monitor</a>	Displays SPAN and RSPAN session information.
<a href="#">show running-config</a>	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: <a href="http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html">http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html</a> Select the <b>Cisco IOS Commands Master List, Release 12.2</b> to navigate to the command.

## mvr (global configuration)

Use the **mvr** global configuration command without keywords to enable the multicast VLAN registration (MVR) feature on the switch. Use the command with keywords to set the MVR mode for a switch, to configure the MVR IP multicast address, to 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 **no** form of this command to return to the default settings.

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

```
no mvr [group ip-address | mode [compatible | dynamic] | querytime | ringmode flood | vlan vlan-id]
```

### Syntax Description

<b>group</b> <i>ip-address</i>	Statically configure an MVR group IP multicast address on the switch. Use the <b>no</b> 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) Configure multiple contiguous MVR group addresses. The range is 1 to 2000. However, if the mode is compatible, the switch allows only 512 groups, even if you enter a value greater than 512. Dynamic mode supports 2000 groups. The default is 1.
<b>mode</b>	(Optional) Specify the MVR mode of operation. The default is compatible mode.
<b>compatible</b>	Set 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.
<b>dynamic</b>	Set MVR mode to allow dynamic MVR membership on source ports.
<b>querytime</b> <i>value</i>	(Optional) Set 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 (one-half) second.  Use the <b>no</b> form of the command to return to the default setting.
<b>ringmode flood</b>	(Optional) Enable MVR ring mode flooding for access rings. Entering this command controls traffic flow in egress ports in a ring environment to prevent the dropping of unicast traffic.
<b>vlan</b> <i>vlan-id</i>	(Optional) Specify the VLAN on which MVR multicast data is 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.

### Defaults

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 5 tenths (one-half) second.

The default multicast VLAN for MVR is VLAN 1.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.
12.2(52)SE	The <b>ringmode flood</b> keywords were added.

### Usage Guidelines

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.

When MVR mode is compatible (the default), you can configure 512 multicast entries (MVR group addresses). Although the range appears in the command line help as 1 to 2000, the switch allows only 512 groups.

When MVR mode is dynamic, you can configure a maximum of 2000 MVR group addresses on the switch. The maximum number of simultaneous active multicast streams (that is, the maximum number of television channels that can be receiving) is 512. When this limit is reached, a message is generated that the *Maximum hardware limit of groups had been reached*. Note that a hardware entry occurs when there is an IGMP join on a port or when you configure a port to join a group by entering the **mvr vlan vlan-id group ip-address** interface configuration command.

MVR supports aliased IP multicast addresses on the switch. However, if the switch is interoperating with Catalyst 3550 or 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 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.

Starting with Cisco IOS release 12.2(52)SE, you can enter the **mvr ringmode flood** global configuration command to ensure that data forwarding in a ring topology is limited to membership detected ports and excludes forwarding to multicast router ports. This prevents unicast traffic from being dropped in a ring environment when MVR multicast traffic is flowing in one direction and unicast traffic is flowing in the other direction.

**Examples**

This example shows how to enable MVR:

```
Switch(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:

```
Switch(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:

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

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

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

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

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

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

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

**Related Commands**

Command	Description
<a href="#">mvr (interface configuration)</a>	Configures MVR ports.
<a href="#">show mvr</a>	Displays MVR global parameters or port parameters.
<a href="#">show mvr interface</a>	Displays the configured MVR interfaces with their type, mode, VLAN, status and Immediate Leave configuration, and can also displays all MVR groups of which the interface is a member.
<a href="#">show mvr members</a>	Displays all ports that are members of an MVR multicast group; if the group has no members, its status is shown as Inactive.

## mvr (interface configuration)

Use the **mvr** interface configuration command to configure a Layer 2 port as a multicast VLAN registration (MVR) receiver or source port, to set the Immediate Leave feature, and to statically assign a port to an IP multicast VLAN and IP address. Use the **no** form of this command to return to the default settings.

```
mvr {immediate | type {receiver | source} | vlan vlan-id {[group ip-address] [receiver vlan vlan-id]}}
```

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

Syntax Description		
<b>immediate</b>	(Optional) Enable the Immediate Leave feature of MVR on a port. Use the <b>no mvr immediate</b> command to disable the feature.	
<b>type</b>	(Optional) Configure 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 <b>no mvr type</b> command resets the port as neither a source or a receiver port.	
<b>receiver</b>	Configure the port as a subscriber port that can only receive multicast data. Receiver ports cannot belong to the multicast VLAN.	
<b>source</b>	Configure 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.  <b>Note</b> When you are configuring a trunk port as an MVR receiver port, we recommend that the source port is configured as a network node interface (NNI) and the MVR trunk receiver port is configured as a user node interface (UNI) or an enhanced network interface (ENI).	
<b>vlan <i>vlan-id</i></b>	Specify the mvr vlan for the system.	
<b>group <i>ip-address</i></b>	(Optional) Statically configure 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 or VLAN is joining.	
<b>receiver vlan <i>vlan-id</i></b>	(Optional) Specify a receiver VLAN.	

### Defaults

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
12.2(44)EY	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 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 gigabitethernet0/1
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 gigabitethernet0/1
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 gigabitethernet0/2
Switch(config-if)# mvr vlan1 group 230.1.23.4
```

This example shows how to add a port 2 on VLAN 100 as a static member of IP multicast group 228.1.23.4. In this example, the receive port is an access port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# mvr vlan 100 group 228.1.23.4
```

This example shows how to add on port 5 the receiver VLAN 201 with an MVR VLAN of 100.

```
Switch(config)# interface fastethernet0/5
Switch(config-if)# mvr vlan 100 receiver vlan 201
```

This example shows how to add on port 5 the receiver VLAN 201 as a static member of the IP multicast group 239.1.1.1, with an MVR VLAN of 100:

```
Switch(config)# interface fastethernet0/5
Switch(config-if)# mvr vlan 100 group 239.1.1.1 receiver vlan 201
```

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

**Related Commands**

Command	Description
<a href="#">mvr (global configuration)</a>	Enables and configures multicast VLAN registration on the switch.
<a href="#">show mvr</a>	Displays MVR global parameters or port parameters.
<a href="#">show mvr interface</a>	Displays the configured MVR interfaces or displays the multicast groups to which a receiver port belongs. Also displays all MVR groups of which the interface is a member.
<a href="#">show mvr members</a>	Displays all receiver ports that are members of an MVR multicast group.

# no authentication logging verbose

Use the **no authentication logging verbose** global configuration command on the switch stack or on a standalone switch to filter detailed information from authentication system messages.

## no authentication logging verbose

**Defaults** All details are displayed in the system messages.

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(55)SE	This command was introduced.

**Usage Guidelines** This command filters details, such as anticipated success, from authentication system messages.

**Examples** To filter verbose authentication system messages:

```
Switch(config)# no authentication logging verbose
```

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

Related Commands	Command	Description
	<b>no authentication logging verbose</b>	Filters details from authentication system messages.
	<b>no dot1x logging verbose</b>	Filters details from 802.1x system messages.
	<b>no mab logging verbose</b>	Filters details from MAC authentication bypass (MAB) system messages.

# no dot1x logging verbose

Use the **no dot1x logging verbose** global configuration command on the switch stack or on a standalone switch to filter detailed information from 802.1x system messages.

**no dot1x logging verbose**

**Defaults** All details are displayed in the system messages.

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(55)SE	This command was introduced.

**Usage Guidelines** This command filters details, such as anticipated success, from 802.1x system messages.

**Examples** To filter verbose 802.1x system messages:

```
Switch(config)# no dot1x logging verbose
```

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

Related Commands	Command	Description
	<b>no authentication logging verbose</b>	Filters details from authentication system messages.
	<b>no dot1x logging verbose</b>	Filters details from 802.1x system messages.
	<b>no mab logging verbose</b>	Filters details from MAC authentication bypass (MAB) system messages.

## no mab logging verbose

Use the **no mab logging verbose** global configuration command on the switch stack or on a standalone switch to filter detailed information from MAC authentication bypass (MAB) system messages.

### no mab logging verbose

#### Defaults

All details are displayed in the system messages.

#### Syntax Description

This command has no arguments or keywords.

#### Command Modes

Global configuration

#### Command History

Release	Modification
12.2(55)SE	This command was introduced.

#### Usage Guidelines

This command filters details, such as anticipated success, from MAC authentication bypass (MAB) system messages.

#### Examples

To filter verbose MAB system messages:

```
Switch(config)# no mab logging verbose
```

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

#### Related Commands

Command	Description
<b>no authentication logging verbose</b>	Filters details from authentication system messages.
<b>no dot1x logging verbose</b>	Filters details from 802.1x system messages.
<b>no mab logging verbose</b>	Filters details from MAC authentication bypass (MAB) system messages.



# oam protocol cfm svlan

Use the **oam protocol cfm svlan** EVC configuration command to configure the Ethernet virtual connection (EVC) operation, administration, and maintenance (OAM) protocol as IEEE 801.2ag Connectivity Fault Management (CFM) and to identify the service provider VLAN-ID for a CFM domain level. Use the **no** form of this command to remove the OAM protocol configuration for the EVC.

```
oam protocol cfm svlan vlan-id domain domain-name
```

```
no oam protocol
```

## Syntax Description

<i>vlan-id</i>	Service provider VLAN ID for CFM. The range is 1 to 4094.
<b>domain</b> <i>domain-name</i>	Identify the CFM domain for the service provider VLAN ID. If the CFM domain does not exist, the command is rejected, and an error message appears.

## Defaults

There are no service provider VLANs identified for an EVC.

## Command Modes

EVC configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

When you enter **domain** *domain-name*, the CFM domain must have already been created by entering the **ethernet cfm domain** *domain-name level level-id* global configuration command. If the CFM domain does not exist, the command is rejected, and an error message appears.

## Examples

This example shows how to enter EVC configuration mode and to configure the OAM protocol as CFM:

```
Switch(config)# ethernet evc test1
Switch(config-vc)# oam protocol cfm svlan 22 domain Operator
```

## Related Commands

Command	Description
<b>ethernet evc</b> <i>evc-id</i>	Defines an EVC and enters EVC configuration mode.
<b>ethernet cfm domain</b>	Defines a CFM domain and sets the domain level.

## pagp learn-method

Use the **pagp learn-method** interface configuration command to learn the source address of incoming packets received from an EtherChannel port. Use the **no** form of this command to return to the default setting.

**pagp learn-method** { aggregation-port | physical-port }

**no pagp learn-method**



### Note

PAGP is available only on network node interfaces (NNIs) and enhanced network interfaces (ENIs).

### Syntax Description

<b>aggregation-port</b>	Specify address learning on the logical port-channel. The switch sends packets to the source using any of the ports in the EtherChannel. This setting is the default. With aggregate-port learning, it is not important on which physical port the packet arrives.
<b>physical-port</b>	Specify address learning on the physical port within the EtherChannel. The switch sends packets to the source using the same port in the EtherChannel from which it learned the source address. The other end of the channel uses the same port in the channel for a particular destination MAC or IP address.

### Defaults

The default is aggregation-port (logical port channel).

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

If the interface is a user network interface (UNI), you must enter the **port-type nni** or **port-type eni** interface configuration command before configuring **pagp learn-method**. Learn must be configured to the same method at both ends of the link.



### Note

The Cisco ME switch supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the command-line interface (CLI). The **pagp learn-method** and the **pagp port-priority** interface configuration commands have no effect on the switch hardware, but they are required for PAGP interoperability with devices that only support address learning by physical ports.

**Note**

When the link partner to the Cisco ME switch is a physical learner, we recommend that you configure the switch as a physical-port learner. Use the **pagp learn-method physical-port** interface configuration command, and set the load-distribution method based on the source MAC address by using the **port-channel load-balance src-mac** global configuration command. Only use the **pagp learn-method** interface configuration command in this situation.

**Examples**

This example shows how to set the learning method to learn the address on the physical port within the EtherChannel:

```
Switch(config-if)# pagp learn-method physical-port
```

This example shows how to set the learning method to learn the address on the port-channel within the EtherChannel:

```
Switch(config-if)# pagp learn-method aggregation-port
```

You can verify your settings by entering the **show running-config** privileged EXEC command or the **show pagp channel-group-number internal** privileged EXEC command.

**Related Commands**

Command	Description
<a href="#">pagp port-priority</a>	Selects a port over which all traffic through the EtherChannel is sent.
<a href="#">show pagp</a>	Displays PAgP channel-group information.
<a href="#">show running-config</a>	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: <a href="http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html">http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html</a> Select the <b>Cisco IOS Commands Master List, Release 12.2</b> to navigate to the command.

## pagp port-priority

Use the **pagp port-priority** interface configuration command to select a port over which all Port Aggregation Protocol (PAgP) traffic through the EtherChannel is sent. If all unused ports in the EtherChannel are in hot-standby mode, they can be placed into operation if the currently selected port and link fails. Use the **no** form of this command to return to the default setting.

**pagp port-priority** *priority*

**no pagp port-priority**



### Note

PAgP is available only on network node interfaces (NNIs) and enhanced network interfaces (ENIs).

### Syntax Description

*priority* A priority number ranging from 0 to 255.

### Defaults

The default is 128.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

If the interface is a user network interface (UNI), you must enter the **port-type nni** or **port-type eni** interface configuration command before configuring **pagp port-priority**.

The physical port with the highest operational priority and that has membership in the same EtherChannel is the one selected for PAgP transmission.



### Note

The Cisco ME switch supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the command-line interface (CLI). The **pagp learn-method** and the **pagp port-priority** interface configuration commands have no effect on the switch hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports.

When the link partner to the Cisco ME switch is a physical learner, we recommend that you configure the switch as a physical-port learner by using the **pagp learn-method physical-port** interface configuration command and to set the load-distribution method based on the source MAC address by using the **port-channel load-balance src-mac** global configuration command. Use the **pagp learn-method** interface configuration command only in this situation.

---

**Examples**

This example shows how to set the port priority to 200:

```
Switch(config-if)# pagp port-priority 200
```

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

---

**Related Commands**

Command	Description
<a href="#">pagp learn-method</a>	Provides the ability to learn the source address of incoming packets.
<a href="#">show pagp</a>	Displays PAgP channel-group information.
<b>show running-config</b>	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: <a href="http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html">http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html</a> Select the <b>Cisco IOS Commands Master List, Release 12.2</b> to navigate to the command.

---

## permit (ARP access-list configuration)

Use the **permit** Address Resolution Protocol (ARP) access-list configuration command to permit an ARP packet based on matches against the Dynamic Host Configuration Protocol (DHCP) bindings. Use the **no** form of this command to remove the specified access control entry (ACE) from the access control list.

```
permit {[request] ip {any | host sender-ip | sender-ip sender-ip-mask} mac {any | host sender-mac | sender-mac sender-mac-mask} | response ip {any | host sender-ip | sender-ip sender-ip-mask} [{any | host target-ip | target-ip target-ip-mask}] mac {any | host sender-mac | sender-mac sender-mac-mask} [{any | host target-mac | target-mac target-mac-mask}] [log]
```

```
no permit {[request] ip {any | host sender-ip | sender-ip sender-ip-mask} mac {any | host sender-mac | sender-mac sender-mac-mask} | response ip {any | host sender-ip | sender-ip sender-ip-mask} [{any | host target-ip | target-ip target-ip-mask}] mac {any | host sender-mac | sender-mac sender-mac-mask} [{any | host target-mac | target-mac target-mac-mask}] [log]
```

### Syntax Description

<b>request</b>	(Optional) Requests a match for the ARP request. When <b>request</b> is not specified, matching is performed against all ARP packets.
<b>ip</b>	Specify the sender IP address.
<b>any</b>	Accept any IP or MAC address.
<b>host</b> <i>sender-ip</i>	Accept the specified sender IP address.
<i>sender-ip</i> <i>sender-ip-mask</i>	Accept the specified range of sender IP addresses.
<b>mac</b>	Specify the sender MAC address.
<b>host</b> <i>sender-mac</i>	Accept the specified sender MAC address.
<i>sender-mac</i> <i>sender-mac-mask</i>	Accept the specified range of sender MAC addresses.
<b>response ip</b>	Define the IP address values for the ARP responses.
<b>host</b> <i>target-ip</i>	(Optional) Accept the specified target IP address.
<i>target-ip target-ip-mask</i>	(Optional) Accept the specified range of target IP addresses.
<b>mac</b>	Specify the MAC address values for the ARP responses.
<b>host</b> <i>target-mac</i>	(Optional) Accept the specified target MAC address.
<i>target-mac</i> <i>target-mac-mask</i>	(Optional) Accept the specified range of target MAC addresses.
<b>log</b>	(Optional) Log a packet when it matches the ACE. Matches are logged if you also configure the <b>matchlog</b> keyword in the <b>ip arp inspection vlan logging</b> global configuration command.

### Defaults

There are no default settings.

### Command Modes

ARP access-list configuration

**Command History**

Release	Modification
12.2(44)EY	This command was introduced.

**Usage Guidelines**

You can add permit clauses to forward ARP packets based on some matching criteria.

**Examples**

This example shows how to define an ARP access list and to permit both ARP requests and ARP responses from a host with an IP address of 1.1.1.1 and a MAC address of 0000.0000.abcd:

```
Switch(config)# arp access-list static-hosts
Switch(config-arp-nacl)# permit ip host 1.1.1.1 mac host 0000.0000.abcd
Switch(config-arp-nacl)# end
```

You can verify your settings by entering the **show arp access-list** privileged EXEC command.

**Related Commands**

Command	Description
<a href="#">arp access-list</a>	Defines an ARP access control list (ACL).
<a href="#">deny (ARP access-list configuration)</a>	Denies an ARP packet based on matches against the DHCP bindings.
<a href="#">ip arp inspection filter vlan</a>	Permits ARP requests and responses from a host configured with a static IP address.
<a href="#">show arp access-list</a>	Displays detailed information about ARP access lists.

## permit (IPv6 access-list configuration)

Use the **permit** IPv6 access list configuration command to set permit conditions for an IPv6 access list. Use the **no** form of this command to remove the permit conditions.

```
permit {protocol} {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator
[port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address}
[operator [port-number]] [dscp value] [fragments] [log] [log-input] [routing] [sequence
value] [time-range name]
```

```
no permit {protocol} {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator
[port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address}
[operator [port-number]] [dscp value] [fragments] [log] [log-input] [routing] [sequence
value] [time-range name]
```



### Note

Although visible in the command-line help strings, the **flow-label** and **reflect** keywords are not supported.

### Internet Control Message Protocol

```
permit icmp {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator
[port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address}
[operator [port-number]] [icmp-type [icmp-code] | icmp-message] [dscp value] [log]
[log-input] [routing] [sequence value] [time-range name]
```

### Transmission Control Protocol

```
permit tcp {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator
[port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address}
[operator [port-number]] [ack] [dscp value] [established] [fin] [log] [log-input] [neq {port |
protocol}] [psh] [range {port | protocol}] [rst] [routing] [sequence value] [syn] [time-range
name] [urg]
```

### User Datagram Protocol

```
permit udp {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator
[port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address}
[operator [port-number]] [dscp value] [log] [log-input] [neq {port | protocol}] [range {port |
protocol}] [routing] [sequence value] [time-range name]
```



### Note

Although visible in the command-line help strings, the **flow-label** and **reflect** keywords are not supported.

This command is available only if your switch has a switch database management (SDM) dual IPv4 and IPv6 template configured.



Syntax Description	
<i>protocol</i>	Name or number of an Internet protocol. It can be one of the keywords <b>ahp</b> , <b>esp</b> , <b>icmp</b> , <b>ipv6</b> , <b>pcp</b> , <b>sctp</b> , <b>tcp</b> , or <b>udp</b> , or an integer in the range from 0 to 255 representing an IPv6 protocol number.
<i>source-ipv6-prefix/prefix-length</i>	The source IPv6 network or class of networks for which to set permit conditions.  This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
<b>any</b>	An abbreviation for the IPv6 prefix <code>::/0</code> .
<b>host</b> <i>source-ipv6-address</i>	The source IPv6 host address for which to set permit conditions.  This <i>source-ipv6-address</i> argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
<i>operator</i> [ <i>port-number</i> ]	(Optional) Specify an operator that compares the source or destination ports of the specified protocol. Operators are <b>lt</b> (less than), <b>gt</b> (greater than), <b>eq</b> (equal), <b>neq</b> (not equal), and <b>range</b> (inclusive range).  If the operator is positioned after the <i>source-ipv6-prefix/prefix-length</i> argument, it must match the source port.  If the operator is positioned after the <i>destination-ipv6-prefix/prefix-length</i> argument, it must match the destination port.  The <b>range</b> operator requires two port numbers. All other operators require one port number.  The optional <i>port-number</i> argument is a decimal number or the name of a TCP or a UDP port. A port number is a number from 0 to 65535. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.
<i>destination-ipv6-prefix/prefix-length</i>	The destination IPv6 network or class of networks for which to set permit conditions.  This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
<b>host</b> <i>destination-ipv6-address</i>	The destination IPv6 host address for which to set permit conditions.  This <i>destination-ipv6-address</i> argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
<b>dscp</b> <i>value</i>	(Optional) Match a differentiated services codepoint value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63.
<b>fragments</b>	(Optional) Match noninitial fragmented packets where the fragment extension header contains a nonzero fragment offset. The <b>fragments</b> keyword is an option only if the protocol is <b>ipv6</b> and the <i>operator</i> [ <i>port-number</i> ] arguments are not specified.

<b>log</b>	(Optional) Send an informational logging message to the console about the packet that matches the entry. (The level of messages logged to the console is controlled by the <b>logging console</b> command.)  The message includes the access list name and sequence number; whether the packet was permitted; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted in the prior 5-minute interval.
<b>log-input</b>	(Optional) Provide the same function as the <b>log</b> keyword, but the logging message also includes the receiving interface.
<b>routing</b>	(Optional) Match packets with the routing extension header.
<b>sequence</b> <i>value</i>	(Optional) Specify the sequence number for the access list statement. The acceptable range is from 1 to 4294967295.
<b>time-range</b> <i>name</i>	(Optional) Specify the time range that applies to the permit statement. The name of the time range and its restrictions are specified by the <b>time-range</b> and <b>absolute</b> or <b>periodic</b> commands, respectively.
<i>icmp-type</i>	(Optional) Specify an ICMP message type for filtering ICMP packets. ICMP packets can be filtered by the ICMP message type. The type is a number from 0 to 255.
<i>icmp-code</i>	(Optional) Specify an ICMP message code for filtering ICMP packets. ICMP packets that are filtered by the ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
<i>icmp-message</i>	(Optional) Specify an ICMP message name for filtering ICMP packets. ICMP packets can be filtered by an ICMP message name or ICMP message type and code. The possible names are listed in the “Usage Guidelines” section.
<b>ack</b>	(Optional) Only for the TCP protocol: acknowledgment (ACK) bit set.
<b>established</b>	(Optional) Only for the TCP protocol: Means the connection has been established. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.
<b>fin</b>	(Optional) Only for the TCP protocol: Fin bit set; no more data from sender.
<b>neq</b> { <i>port</i>   <i>protocol</i> }	(Optional) Match only packets that are not on a given port number.
<b>psh</b>	(Optional) Only for the TCP protocol: Push function bit set.
<b>range</b> { <i>port</i>   <i>protocol</i> }	(Optional) Match only packets in the range of port numbers.
<b>rst</b>	(Optional) Only for the TCP protocol: Reset bit set.
<b>syn</b>	(Optional) Only for the TCP protocol: Synchronize bit set.
<b>urg</b>	(Optional) Only for the TCP protocol: Urgent pointer bit set.

**Defaults**

No IPv6 access list is defined.

**Command Modes**

IPv6 access-list configuration

**Command History**

Release	Modification
12.2(50)SE	This command was introduced.

**Usage Guidelines**

The **permit** (IPv6 access-list configuration mode) command is similar to the **permit** (IPv4 access-list configuration mode) command, but it is IPv6-specific.

Use the **permit** (IPv6) command after the **ipv6 access-list** command to enter IPv6 access-list configuration mode and to define the conditions under which a packet passes the access list.

Specifying IPv6 for the *protocol* argument matches against the IPv6 header of the packet.

By default, the first statement in an access list is number 10, and the subsequent statements increment by 10.

You can add **permit**, **deny**, or **remark** statements to an existing access list without re-entering the entire list. To add a new statement somewhere other than at the end of the list, create a new statement with an appropriate entry number that falls between two existing entry numbers to show where it belongs.

See the **ipv6 access-list** command for more information on defining IPv6 ACLs.

Every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. The two **permit** conditions allow ICMPv6 neighbor discovery. To disallow ICMPv6 neighbor discovery and to deny **icmp any any nd-na** or **icmp any any nd-ns**, there must be an explicit **deny** entry in the ACL. For the three implicit statements to take effect, an IPv6 ACL must contain at least one entry.

The IPv6 neighbor discovery process uses the IPv6 network layer service. Therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, uses a separate data link layer protocol. Therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Both the *source-ipv6-prefix/prefix-length* and *destination-ipv6-prefix/prefix-length* arguments are used for traffic filtering (the *source* prefix filters traffic based upon its source; the *destination* prefix filters traffic based upon its destination).

The switch supports IPv6 address matching for a full range of prefix-lengths.

The **fragments** keyword is an option only if the *operator* [*port-number*] arguments are not specified.

This is a list of ICMP message names:

beyond-scope	destination-unreachable
echo-reply	echo-request
header	hop-limit
mld-query	mld-reduction
mld-report	nd-na
nd-ns	next-header
no-admin	no-route
packet-too-big	parameter-option
parameter-problem	port-unreachable
reassembly-timeout	renum-command

renum-result	renum-seq-number
router-advertisement	router-renumbering
router-solicitation	time-exceeded
unreachable	

## Examples

This example configures two IPv6 access lists named OUTBOUND and INBOUND and applies both access lists to outbound and inbound traffic on a Layer 3 interface. The first and second permit entries in the OUTBOUND list permit all TCP and UDP packets from network 2001:0DB8:0300:0201::/64 to leave the interface. The deny entry in the OUTBOUND list prevents all packets from the network FE80:0:0:0201::/64 (packets that have the link-local prefix FE80:0:0:0201 as the first 64 bits of their source IPv6 address) from leaving the interface. The third permit entry in the OUTBOUND list permits all ICMP packets to leave the interface.

The permit entry in the INBOUND list permits all ICMP packets to enter the interface.

```
Switch(config)#ipv6 access-list OUTBOUND
Switch(config-ipv6-acl)# permit tcp 2001:0DB8:0300:0201::/64 any
Switch(config-ipv6-acl)# permit udp 2001:0DB8:0300:0201::/64 any
Switch(config-ipv6-acl)# deny FE80:0:0:0201::/64 any
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# exit
Switch(config)#ipv6 access-list INBOUND
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# exit
Switch(config)# interface gigabitethernet0/3
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter OUTBOUND out
Switch(config-if)# ipv6 traffic-filter INBOUND in
```



### Note

Given that a **permit any any** statement is not included as the last entry in the OUTBOUND or the INBOUND access list, only TCP, UDP, and ICMP packets can leave or enter the interface (the implicit deny-all condition at the end of the access list denies all other packet types on the interface).

## Related Commands

Command	Description
<a href="#">ipv6 access-list</a>	Defines an IPv6 access list and enters IPv6 access list configuration mode.
<a href="#">ipv6 traffic-filter</a>	Filters incoming or outgoing IPv6 traffic on an interface.
<a href="#">deny (IPv6 access-list configuration)</a>	Sets deny conditions for an IPv6 access list.
<a href="#">show ipv6 access-list</a>	Displays the contents of all current IPv6 access lists.

## permit (MAC access-list configuration)

Use the **permit** MAC access-list configuration command to allow non-IP traffic to be forwarded if the conditions are matched. Use the **no** form of this command to remove a permit condition from the extended MAC access list.

```
{permit | deny} {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr |
dst-MAC-addr mask} [type mask | cos cos | aarp | amber | dec-spanning | decnet-iv |
diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | lsap lsap mask | mop-console |
mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp]
```

```
no {permit | deny} {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr |
dst-MAC-addr mask} [type mask | cos cos | aarp | amber | dec-spanning | decnet-iv |
diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | lsap lsap mask | mop-console |
mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp]
```



### Note

Though visible in the command-line help strings, **appletalk** is not supported as a matching condition.

### Syntax Description

<b>any</b>	Keyword to specify to deny any source or destination MAC address.
<b>host</b> <i>src-MAC-addr</i>   <i>src-MAC-addr mask</i>	Define 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.
<b>host</b> <i>dst-MAC-addr</i>   <i>dst-MAC-addr mask</i>	Define 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) Use 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"> <li><i>type</i> is 0 to 65535, specified in hexadecimal.</li> <li><i>mask</i> is a mask of <i>don't care</i> bits applied to the Ethertype before testing for a match.</li> </ul>
<b>aarp</b>	(Optional) Select Ethertype AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
<b>amber</b>	(Optional) Select EtherType DEC-Amber.
<b>cos</b> <i>cos</i>	(Optional) Select 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 <b>cos</b> option is configured.
<b>dec-spanning</b>	(Optional) Select EtherType Digital Equipment Corporation (DEC) spanning tree.
<b>decnet-iv</b>	(Optional) Select EtherType DECnet Phase IV protocol.
<b>diagnostic</b>	(Optional) Select EtherType DEC-Diagnostic.
<b>dsm</b>	(Optional) Select EtherType DEC-DSM.
<b>etype-6000</b>	(Optional) Select EtherType 0x6000.
<b>etype-8042</b>	(Optional) Select EtherType 0x8042.
<b>lat</b>	(Optional) Select EtherType DEC-LAT.
<b>lavc-sca</b>	(Optional) Select EtherType DEC-LAVC-SCA.

<b>lsap</b> <i>lsap-number mask</i>	(Optional) Use 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 <i>don't care</i> bits applied to the LSAP number before testing for a match.
<b>mop-console</b>	(Optional) Select EtherType DEC-MOP Remote Console.
<b>mop-dump</b>	(Optional) Select EtherType DEC-MOP Dump.
<b>msdos</b>	(Optional) Select EtherType DEC-MSDOS.
<b>mumps</b>	(Optional) Select EtherType DEC-MUMPS.
<b>netbios</b>	(Optional) Select EtherType DEC- Network Basic Input/Output System (NETBIOS).
<b>vines-echo</b>	(Optional) Select EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
<b>vines-ip</b>	(Optional) Select EtherType VINES IP.
<b>xns-idp</b>	(Optional) Select EtherType Xerox Network Systems (XNS) protocol suite.

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 [Table 2-3](#).

**Table 2-3** 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

### Defaults

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
12.2(44)EY	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 **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.

**Note**

For more information about MAC-named extended access lists, see the software configuration guide for this release.

**Examples**

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.

```
Switch(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:

```
Switch(config-ext-macl)# no permit any 00c0.00a0.03fa 0000.0000.0000 netbios
```

This example permits all packets with Ethertype 0x4321:

```
Switch(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
<a href="#">deny (MAC access-list configuration)</a>	Denies non-IP traffic to be forwarded if conditions are matched.
<a href="#">mac access-list extended</a>	Creates an access list based on MAC addresses for non-IP traffic.
<a href="#">show access-lists</a>	Displays access control lists configured on a switch.

# police

Use the **police** policy-map class configuration command to define an individual policer for classified traffic and to enter policy-map class police configuration mode. A policer defines a maximum permissible rate of transmission, a maximum burst size and an excess burst size for transmissions, and an action to take if a maximum is exceeded. In policy-map class police configuration mode, you can specify multiple actions for a packet. Use the **no** form of this command to remove a policer.


**Note**

Although visible in the command-line help, the **police rate** and **percent** keywords are not supported.

```
police { cir cir-bps | rate-bps } [burst-bytes] | bc [burst-value] | pir pir-bps [be burst-bytes]
  [conform-action [drop | set-cos-transmit {new-cos-value | [cos | dscp | precedence] [table
table-map name]} | set-dot1ad-dei-transmit {new-dei-value | [cos | dscp | precedence] [table
table-map name]} | set-dscp-transmit {new-dscp-value | [cos | dscp | precedence] [table
table-map name]} | set-prec-transmit {new-precedence-value | [cos | dscp | precedence]
[table table-map name]} | set-qos-transmit qos-group-value | transmit] [exceed action [drop
| set-cos-transmit {new-cos-value | [cos | dscp | precedence] [table table-map name]} |
set-dot1ad-dei-transmit {new-dei-value | [cos | dscp | precedence] [table table-map name]} |
set-dscp-transmit {new-dscp-value | [cos | dscp | precedence] [table table-map name]} |
set-prec-transmit {new-precedence-value | [cos | dscp | precedence] [table table-map name]}
| set-qos-transmit qos-group-value | transmit] [violate-action [drop | set-cos-transmit
{new-cos-value | [cos | dscp | precedence] [table table-map name]} | set-dot1ad-dei-transmit
{new-dei-value | [cos | dscp | precedence] [table table-map name]} | set-dscp-transmit
{new-dscp-value | [cos | dscp | precedence] [table table-map name]} | set-prec-transmit
{new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-qos-transmit
qos-group-value | transmit]]
```

```
no police { cir cir-bps | rate-bps } [burst-bytes] | bc [burst-value] | pir pir-bps [be burst-bytes]
  [conform-action [drop | set-cos-transmit {new-cos-value | [cos | dscp | precedence] [table
table-map name]} | set-dot1ad-dei-transmit {new-dei-value | [cos | dscp | precedence] [table
table-map name]} | set-dscp-transmit {new-dscp-value | [cos | dscp | precedence] [table
table-map name]} | set-prec-transmit {new-precedence-value | [cos | dscp | precedence]
[table table-map name]} | set-qos-transmit qos-group-value | transmit] [exceed action [drop
| set-cos-transmit {new-cos-value | [cos | dscp | precedence] [table table-map name]} |
set-dot1ad-dei-transmit {new-dei-value | [cos | dscp | precedence] [table table-map name]} |
set-dscp-transmit {new-dscp-value | [cos | dscp | precedence] [table table-map name]} |
set-prec-transmit {new-precedence-value | [cos | dscp | precedence] [table table-map name]}
| set-qos-transmit qos-group-value | transmit] [violate-action [drop | set-cos-transmit
{new-cos-value | [cos | dscp | precedence] [table table-map name]} | set-dot1ad-dei-transmit
{new-dei-value | [cos | dscp | precedence] [table table-map name]} | set-dscp-transmit
{new-dscp-value | [cos | dscp | precedence] [table table-map name]} | set-prec-transmit
{new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-qos-transmit
qos-group-value | transmit]]
```


**Note**

When **police** is used with the **priority** policy-map class command for unconditionally rate-limiting the priority queue, burst size values are not supported, and the *rate-bps* range is smaller. Only the default conform-action of **transmit** and the default exceed-action of **drop** are supported.



Syntax	Description
<b>cir</b>	Committed information rate (CIR) used for policing traffic.
<i>cir-bps</i>	CIR rate in bps. The range is 8000 to 1000000000 bps. <b>Note</b> The range for <b>police</b> with the <b>priority</b> command for output service policies is 64000 to 1000000000.
<i>rate-bps</i>	Specify the average traffic rate in b/s. The range is 8000 to 1000000000. <b>Note</b> The range for <b>police</b> with the <b>priority</b> command for output service policies is 64000 to 1000000000.
<i>burst-bytes</i>	(Optional) Specify the normal burst size in bytes. The range is 8000 to 1000000.
<b>bc</b> [ <i>burst-value</i> ]	(Optional) Conform burst. The number of acceptable burst bytes. The range is 8000 to 1000000 bytes.  If no burst value is entered, the system calculates a burst value that equals the number of bytes that can be sent in 250 milliseconds (ms) at the CIR rate. In most cases, the automatically calculated value is appropriate; enter a new value only if you are aware of all implications.
<b>pir</b> <i>pir-bps</i>	(Optional) Peak information rate (PIR) used for policing traffic. The range is from 8000 to 1000000000 b/s.
<b>be</b> <i>burst-bytes</i>	(Optional) Exceed burst. The number of acceptable exceed burst bytes. The range is 8000 to 1000000 bytes.
<b>conform-action</b>	(Optional) Action to be taken for packets that conform to (are less than or equal to) the CIR.
<b>drop</b>	(Optional) Drop the packet. <b>Note</b> If the conform action is set to <b>drop</b> , the exceed and violate actions are automatically set to <b>drop</b> . If the exceed action is set to <b>drop</b> , the violate action is automatically set to <b>drop</b> .
<b>set-cos-transmit</b> <i>new-cos-value</i>	Set a new class of service (CoS) value for the packet and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new CoS value is 0 to 7.
<b>set-dot1ad-dei-transmit</b> <i>new-dei-value</i>	Set a new drop eligibility indicator (DEI) value in the IEEE 802.1ad frame for the packet, and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new DEI value is 0 to 1. The DEI value applies only to 802.1ad ports.
<b>set-dscp-transmit</b> <i>new-dscp-value</i>	Set a new Differentiated Services Code Point (DSCP) value for the packet, and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new DSCP value is 0 to 63.
<b>set-prec-transmit</b> <i>new-precedence-value</i>	Set a new IP precedence value for the packet, and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new IP precedence value is 0 to 7.
<b>set-qos-transmit</b> <i>qos-group-value</i>	Set a new quality of service (QoS) group value for the packet, and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new QoS value is 0 to 99.
<b>cos</b>	(Optional) Set the packet marking specified in the preceding keyword based on the CoS value of the incoming packet, and send the packet. This specifies the <i>from-type</i> of the enhanced packet-marking action.

<b>dscp</b>	(Optional) Set the packet marking specified in the preceding keyword based on the DSCP value of the incoming packet, and send the packet. This specifies the <i>from-type</i> of the enhanced packet-marking action.
<b>precedence</b>	(Optional) Set the packet marking specified in the preceding keyword based on the IP precedence value of the incoming packet, and send the packet. This specifies the <i>from-type</i> of the enhanced packet-marking action.
<b>table</b> <i>table-map name</i>	(Optional) Used with the preceding <i>from-type</i> keyword. Specify the table map to be used for the enhanced packet marking. The <i>to-type</i> of the action is marked based on the <i>from-type</i> parameter of the action using this table map.
<b>transmit</b>	(Optional) Send the packet unmodified.
<b>exceed-action</b>	(Optional) Action to be taken for packets that exceed the CIR but are less than or equal to the PIR.
<b>violate-action</b>	(Optional) Action to be taken for packets exceed the PIR.

**Defaults**

No policers are defined. Conform burst (**bc**) is automatically configured to 250 ms at the configured CIR.

**Command Modes**

Policy-map class configuration

**Command History**

Release	Modification
12.2(44)EY	This command was introduced.
12.2(55)SE	The <b>set-dot1ad-dei-transmit</b> keywords were added.

**Usage Guidelines**

You can configure conform-action marking by using enhanced packet marking and configure exceed-action to send the packet unmodified, mark using explicit values, and use all combinations of enhanced packet marking. Enhanced packet marking modifies a QoS marking based on any incoming QoS marking and table maps. The switch also supports marking multiple QoS parameters for the same class and simultaneously configuring conform-action, exceed-action, and violate-action marking.

If the conform action is set to **drop**, the exceed and violate actions are automatically set to **drop**. If the exceed action is set to **drop**, the violate action is automatically set to **drop**.

The switch supports a maximum of 254 policer profiles. The number of supported policer instances is 1024 minus 1 more than the total number of interfaces on the switch. You can apply the same profile in multiple instances.

- You can specify 256 *unique* VLAN classification criteria within a per-port, per-VLAN policy-map, across all ports on the switch. Any policy attachment or change that causes this limit to be exceeded fails with a *VLAN label resources exceeded* error message.
- You can attach per-port and per-port, per-VLAN policy-maps across all ports on the switch until QoS ACE classification resource limitations are reached. Any policy attachment or change that causes this limit to be exceeded fails with a *TCAM resources exceeded* error message.

- When CPU protection is enabled, you can configure only 45 policers per port. You can configure up to 64 policers per port by disabling CPU protection by entering the **no policer cpu uni all** global configuration command, and reloading the switch allows. You can enter the **show policer cpu uni-eni {drop | rate}** privileged EXEC command to see if CPU protection is enabled. For more information, see the **policer cpu uni** command.
- Note these limitations when you disable CPU protection:
  - When CPU protection is disabled, you can configure a maximum of 63 policers per port (62 on every fourth port) for user-defined classes and one for class-default for all switches. Any policy attachment or change that causes this limit to be exceeded fails with a *policer resources exceeded* error message.
  - When CPU protection is disabled, you can configure 255 policers on the switch for platform. Any policy attachment or change that causes this limit to be exceeded fails with a *policer resources exceeded* error message.
  - If you disable CPU protection and attach a policy map with more than 45 policers, and enable CPU protection again, and then reload, 19 policers per port are again required for CPU protection. During reload, the policers 46 and above will reach the *policer resources exceeded* error condition, and no policers are attached to those classes.

Policing is only supported in input policies or in output policies that were configured with the **priority** policy-map class configuration command to reduce bandwidth in the priority queue.


**Note**

When used with the **priority** command in an output policy, the police rate range is 64000 to 1000000000 bps, even though the range that appears in the command-line interface help is 8000 to 1000000000. You cannot attach an output service policy with an out-of-range rate.

An output policy map should match only the modified values of the out-of-profile traffic and not the original values.

Only 802.1ad S-UNI and S-NNI ports can use policers marking the DEI bit.

To configure multiple conform-actions or multiple exceed-actions, enter policy-map class police configuration mode, and use the **conform-action**, **exceed-action**, and **violate-action** policy-map class police configuration commands.

If you do not configure a **violate-action**, by default the violate class is assigned the same action as the exceed action.

When you define the policer and press Enter, you enter policy-map class police configuration mode, in which you can configure multiple policing actions:

- **conform-action**: the action to be taken on packets that conform to (are less than or equal to) the CIR. The default action is to **transmit** the packet. For more information, see the **conform-action** policy-map class police command.
- **exceed-action**: the action to be taken on packets that exceed the CIR but are less than or equal to the PIR. The default action is to **drop** the packet. For more information, see the **exceed-action** policy-map class police command.
- **violate-action**: the action to be taken on packets that exceed the PIR. The default action is to **drop** the packet. For more information, see the **violate-action** policy-map class police command.
- **exit**: exits from QoS policy-map class police configuration mode. If you do not want to set multiple actions, you can enter **exit** without entering any other policy-map class police commands.
- **no**: negates or sets the default values of a command.

**Examples**

This example shows how to configure a policer with a 1-Mb/s average rate with a burst size of 20 KB. The policer sets a new DSCP precedence value if the packets conform to the rate and drops the packet if traffic exceeds the rate.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class inclass1
Switch(config-pmap-c)# police cir 1000000 20000 conform-action set-dscp-transmit 46
exceed-action drop
Switch(config-pmap-c)# exit
```

This example shows how to configure 2-rate, 3-color policing by using policy-map configuration mode.

```
Switch(config)# class-map cos-4
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
Switch(config)# policy-map in-policy
Switch(config-pmap)# class cos-4
Switch(config-pmap-c)# police cir 5000000 pir 8000000 conform-action transmit
exceed-action set-dscp-transmit 24 violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input in-policy
Switch(config-if)# exit
```

This example shows how to create the same configuration by using policy-map class police configuration mode.

```
Switch(config)# class-map cos-4
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
Switch(config)# policy-map in-policy
Switch(config-pmap)# class cos-4
Switch(config-pmap-c)# police cir 5000000 pir 8000000
Switch(config-pmap-c-police)# conform-action transmit
Switch(config-pmap-c-police)# exceed-action set-dscp-transmit 24
Switch(config-pmap-c-police)# violate-action drop
Switch(config-pmap-c-police)# end
```

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

**Related Commands**

Command	Description
<a href="#">class</a>	Defines a traffic classification match criteria for the specified class-map name.
<a href="#">conform-action</a>	Defines multiple actions for a policy-map class for packets that meet the CIR or PIR and have a rate less than the conform burst.
<a href="#">exceed-action</a>	Defines multiple actions for a policy-map class for packets that exceed the CIR or PIR and with a rate between the conform value and the exceed burst.
<a href="#">policy-map</a>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
<a href="#">violate-action</a>	Defines multiple actions for a policy-map class for packets that exceed the CIR and PIR with a rate that exceeds the conform rate plus the exceed burst.
<a href="#">show policy-map</a>	Displays QoS policy maps.

## policer aggregate (global configuration)

Use the **policer aggregate** global configuration command to create an aggregate policer to police all traffic across multiple classes in an input policy map. An aggregate policer can be shared by multiple classes in the same policy map. A policer defines a maximum permissible rate of transmission or committed information rate, a maximum burst size for transmissions, and an action to take if the maximum is met or exceeded. Use the **no** form of this command to remove the specified policer.

```
policer aggregate aggregate-policer-name {rate-bps | cir cir-bps} [bc burst-value]| [pir pir-bps
bc burst-bytes] [conform-action [drop | set-cos-transmit {new-cos-value | [cos | dscp |
precedence] [table table-map name]}] | set-dot1ad-dei-transmit {new-dei-value | [cos | dscp |
precedence] [table table-map name]}] | set-dscp-transmit {new-dscp-value | [cos | dscp |
precedence] [table table-map name]}] | set-prec-transmit {new-precedence-value | [cos | dscp |
precedence] [table table-map name]}] | set-qos-transmit qos-group-value | transmit]
exceed-action [drop | set-cos-transmit {new-cos-value | [cos | dscp | precedence] [table
table-map name]}] | set-dot1ad-dei-transmit {new-dei-value | [cos | dscp | precedence] [table
table-map name]}] | set-dscp-transmit {new-dscp-value | [cos | dscp | precedence] [table
table-map name]}] | set-prec-transmit {new-precedence-value | [cos | dscp | precedence]
[table table-map name]}] | set-qos-transmit qos-group-value | transmit] [violate-action [drop
| set-cos-transmit {new-cos-value | [cos | dscp | precedence]}] | set-dot1ad-dei-transmit
{new-dei-value | [cos | dscp | precedence] [table table-map name]}] | set-dscp-transmit
{new-dscp-value | [cos | dscp | precedence]}] | set-prec-transmit {new-precedence-value | [cos
| dscp | precedence]}] | set-qos-transmit qos-group-value | transmit]]
```

```
no policer aggregate aggregate-policer-name {rate-bps | cir cir-bps} [bc burst-value]| [pir pir-bps
bc burst-bytes] [conform-action [drop | set-cos-transmit {new-cos-value | [cos | dscp |
precedence] [table table-map name]}] | set-dot1ad-dei-transmit {new-dei-value | [cos | dscp |
precedence] [table table-map name]}] | set-dscp-transmit {new-dscp-value | [cos | dscp |
precedence] [table table-map name]}] | set-prec-transmit {new-precedence-value | [cos | dscp |
precedence] [table table-map name]}] | set-qos-transmit qos-group-value | transmit]
exceed-action [drop | set-cos-transmit {new-cos-value | [cos | dscp | precedence] [table
table-map name]}] | set-dot1ad-dei-transmit {new-dei-value | [cos | dscp | precedence] [table
table-map name]}] | set-dscp-transmit {new-dscp-value | [cos | dscp | precedence] [table
table-map name]}] | set-prec-transmit {new-precedence-value | [cos | dscp | precedence]
[table table-map name]}] | set-qos-transmit qos-group-value | transmit] [violate-action [drop
| set-cos-transmit {new-cos-value | [cos | dscp | precedence]}] | set-dot1ad-dei-transmit
{new-dei-value | [cos | dscp | precedence] [table table-map name]}] | set-dscp-transmit
{new-dscp-value | [cos | dscp | precedence]}] | set-prec-transmit {new-precedence-value | [cos
| dscp | precedence]}] | set-qos-transmit qos-group-value | transmit]]
```

### Syntax Description

<i>aggregate-policer-name</i>	Name of the aggregate policer.
<i>rate-bps</i>	Specify the average traffic rate in bits per second (b/s). The range is 8000 to 1000000000.
<b>cir</b> <i>cir-bps</i>	Committed information rate (CIR) in bits/ second. The range is 8000 to 1000000000 b/s.

<b>bc</b> <i>burst- value</i>	(Optional) Conform burst. The number of acceptable burst bytes. The range is 8000 to 1000000 bytes.  If no burst value is entered, the system calculates a burst value that equals the number of bytes that can be sent in 250 milliseconds (ms) at the CIR rate. In most cases, the automatically calculated value is appropriate. Enter a new value only if you are aware of all implications.
<b>pir</b> <i>pir-bps</i>	(Optional) Peak information rate (PIR) used for policing traffic. The range is from 8000 to 1000000000 b/s.
<b>be</b> <i>burst-bytes</i>	(Optional) Exceed burst. The number of acceptable exceed burst bytes. The range is 8000 to 1000000 bytes.
<b>conform-action</b>	(Optional) Action to be taken on packets that meet (are less than or equal to) the CIR.
<b>drop</b>	(Optional) Drop the packet.  <b>Note</b> If the conform action is set to <b>drop</b> , the exceed and violate actions are automatically set to <b>drop</b> . If the exceed action is set to <b>drop</b> , the violate action is automatically set to <b>drop</b> .
<b>set-cos-transmit</b> <i>cos-value</i>	Set a new class of service (CoS) value for the packet, and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new CoS value is 0 to 7.
<b>set-dot1ad-dei-transmit</b> <i>new-dei-value</i>	Set a new drop eligibility indicator (DEI) value in the IEEE 802.1ad frame for the packet, and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new DEI value is 0 to 1. The DEI value applies only to 802.1ad ports.
<b>set-dscp-transmit</b> <i>dscp-value</i>	Set a new Differentiated Services Code Point (DSCP) value for the packet, and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new DCSP value is 0 to 63.
<b>set-prec-transmit</b> <i>precedence-value</i>	Set a new IP precedence value for the packet and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new IP precedence value is 0 to 7.
<b>set-qos-transmit</b> <i>qos-group-value</i>	Set a new quality of service (QoS) group value for the packet and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new QoS value is 0 to 99.
<b>cos</b>	(Optional) Set the packet marking specified in the preceding keyword based on the CoS value of the incoming packet, and send the packet. This specifies the <i>from-type</i> of the enhanced packet-marking action.
<b>dscp</b>	(Optional) Set the packet marking specified in the preceding keyword based on the DSCP value of the incoming packet, and send the packet. This specifies the <i>from-type</i> of the enhanced packet-marking action.
<b>precedence</b>	(Optional) Set the packet marking specified in the preceding keyword based on the IP precedence value of the incoming packet, and send the packet. This specifies the <i>from-type</i> of the enhanced packet-marking action.
<b>table</b> <i>table-map name</i>	(Optional) Used in conjunction with the preceding <i>from-type</i> keyword. Specify the table map to be used for the enhanced packet marking. The <i>to-type</i> of the action is marked based on the <i>from-type</i> parameter of the action using this table map.  Table maps are not supported for violate-actions.

<b>transmit</b>	(Optional) Send the packet unmodified.
<b>exceed-action</b>	(Optional) Action to be taken for packets that exceed the CIR but are less than or equal to the PIR.
<b>violate-action</b>	(Optional) Action to be taken for packets that exceed the PIR.

**Defaults**

No aggregate policers are defined.

When you configure an aggregate policer, conform burst (**bc**) is automatically configured at 250 ms at the configured CIR.

**Command Modes**

Global configuration

**Command History**

Release	Modification
12.2(44)EY	This command was introduced.
12.2(55)SE	The <b>set-dot1ad-dei-transmit</b> keywords were added.

**Usage Guidelines**

You can configure conform-action marking using enhanced packet marking and configure exceed-action and violate-action to send the packet unmodified, mark using explicit values, and use all combinations of enhanced packet marking. Enhanced packet marking modifies a QoS marking based on any incoming QoS marking and table maps. The switch also supports marking multiple QoS parameters for the same class, and simultaneously configuring conform-action, exceed-action, and violate-action marking.

If the conform action is set to **drop**, the exceed and violate actions are automatically set to **drop**. If the exceed action is set to **drop**, the violate action is automatically set to **drop**.

If you do not configure a **violate-action**, by default the violate class is assigned the same action as the **exceed-action**.

The switch supports a maximum of 254 unique aggregate policers.

Aggregate policing is supported only in input policy maps.

Table maps are not supported for **violate-action** for aggregate policing unless a table map is configured for **exceed-action** and no explicit action is configured for violate action.

You can simultaneously configure multiple conform, exceed, and violate actions for an aggregate policer as parameters in the **policer aggregate** global configuration command, but you must enter the actions in this order:

- **conform-action** must be followed by **drop** or **transmit** or by **set** actions in this order:

**set-qos-transmit**

**set-dscp-transmit** or **set-prec-transmit**

**set-cos-transmit**

- **exceed-action** must be followed by **drop** or **transmit** or by **set** actions in this order:

**set-qos-transmit**

**set-dscp-transmit** or **set-prec-transmit**

**set-cos-transmit**

- **violate-action** must be followed by **drop** or **transmit** or by **set** actions in this order:

**set-qos-transmit**

**set-dscp-transmit** or **set-prec-transmit**

**set-cos-transmit**

An output policy map should match only the modified values of the out-of-profile traffic and not the original values.

Only 802.1ad S-UNI and S-NNI ports can use policers marking the DEI bit.

When you configure an aggregate policer, you can configure specific burst sizes and conform and exceed actions. If burst size (**bc**) is not specified, the system calculates an appropriate burst size value that equals the number of bytes that can be sent in 250 ms at the CIR rate. In most cases, the automatically calculated value is appropriate. Enter a new value only if you are aware of all implications.

## Examples

This example shows how to configure an aggregate policer named *agg-pol-1* and attach it to multiple classes within a policy map:

```
Switch(config)# policer aggregate agg-pol-1 10900000 80000 exceed-action drop
Switch(config)# class-map test1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map test2
Switch(config-cmap)# match access-group 2
Switch(config-cmap)# exit
Switch(config)# policy map testexample
Switch(config-pmap)# class test1
Switch(config-pmap-c)# police aggregate agg-pol-1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class test2
Switch(config-pmap-c)# police aggregate agg-pol-1
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input testexample
Switch(config-if)# exit
```

This example shows how to create a 2-rate, 3-color aggregate policer and attach it to multiple classes within a policy map. The policy map is attached to an ingress port.

```
Switch(config)# policer aggregate example cir 10900000 pir 80000000 conform-action
transmit exceed-action drop violate-action drop
Switch(config)# class-map testclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map testclass2
Switch(config-cmap)# match access-group 2
Switch(config-cmap)# exit
Switch(config)# policy-map testexample
Switch(config-pmap)# class testclass
Switch(config-pmap-c)# police aggregate example
Switch(config-pmap-c)# exit
Switch(config-pmap)# class testclass2
Switch(config-pmap-c)# police aggregate example
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input testexample
Switch(config-if)# exit
```



You can verify your settings by entering the **show aggregate-policer** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">class</a>	Defines a traffic classification match criteria for the specified class-map name.
	<a href="#">policy-map</a>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
	<a href="#">show policer aggregate</a>	Displays the aggregate policer configuration.

## police aggregate (policy-map class configuration)

Use the **police aggregate** policy-map class configuration command to apply an aggregate policer to multiple classes in the same policy map. 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. Use the **no** form of this command to remove the specified policer.

**police aggregate** *aggregate-policer-name*

**no police aggregate** *aggregate-policer-name*

<b>Syntax Description</b>	<i>aggregate-policer-name</i> Name of the aggregate policer.
---------------------------	--

<b>Defaults</b>	No aggregate policers are defined.
-----------------	------------------------------------

<b>Command Modes</b>	Policy-map class configuration
----------------------	--------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

<b>Usage Guidelines</b>	<p>The switch supports a maximum of 229 policer instances associated with ports (228 user-configurable policers and 1 policer reserved for internal use). When CPU protection is enabled (the default), you can configure 45 ingress policers per port. If you disable CPU protection by entering the <b>no policer cpu uni all</b> global configuration command and reloading the switch, you can configure up to 64 ingress policers per port (63 policers on every fourth port). For more information, see the <b>policer cpu uni</b> command.</p>
-------------------------	---

Aggregate policing applies only to input policy maps.

An aggregate policer differs from an individual policer in that it is shared by multiple traffic classes within a policy map. You use an aggregate policer to police traffic streams across multiple classes in a policy map attached to an interface. You cannot use aggregate policing to aggregate traffic streams across multiple interfaces.

Only one policy map can use any specific aggregate policer.

<b>Examples</b>	This example shows how to configure the aggregate policing with default actions and apply it across all classes on the same port:
-----------------	---

```
Switch(config)# policy-map inpolicy
Switch(config-pmap)# class in-class1
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class in-class2
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class in-class3
Switch(config-pmap-c)# police aggregate agg_policer1
```

```
Switch(config-pmap-c) # exit
```

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">class</a>	Defines a traffic classification match criteria for the specified class-map name.
<a href="#">policy-map</a>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
<a href="#">show policer aggregate</a>	Displays the aggregate policer configuration.

## policer cpu uni

Use the **policer cpu uni** global configuration command to enable or disable CPU protection and to configure the CPU policing threshold for all user network interfaces (UNIs) and enhanced network interfaces (ENIs) on the switch. Use the **no** form of this command to return to the default rate or to disable CPU protection.

```
policer cpu uni {all | rate-bps}
```

```
no policer cpu uni {all | rate-bps}
```

Syntax Description	all	rate-bps
	Enter this keyword to enable or disable CPU protection. Disabling CPU protection allows 64 policers per port instead of 45.	Specify the CPU policing threshold in bits per second (b/s). The range is 8000 to 409500.

**Defaults** CPU protection is enabled. The default policing threshold is 160000 b/s.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.
	12.2(50)SE	The <b>all</b> keyword was added for disabling or enabling CPU protection.

**Usage Guidelines** To protect against accidental or intentional CPU overload, the switch automatically provides CPU protection or control-plane security by dropping or rate-limiting a predefined set of Layer 2 control packets and some Layer 3 control packets for UNIs and ENIs. The switch pre-allocates 27 control-plane security policers for CPU protection, numbered 0 to 26. A policer of 26 means a drop policer. A policer value of 0 to 25 means that the port uses a rate-limiting policer for the control protocol.

CPU policers are pre-allocated. You can configure only the rate-limiting threshold by using the **policer cpu uni rate-bps** command. The configured threshold applies to all control protocols and all UNIs and ENIs.

CPU protection policing uses 19 policers per port, which allows attaching a maximum of 45 ingress policers to a port. If you need more than 45 policers on a port, you can disable CPU protection by entering the **no cpu policer uni all** global configuration command before you attach a policy map with more than 45 policers. When CPU protection is disabled, you can attach up to 64 ingress policers to a port.

Note these limitations when you disable CPU protection:

- When CPU protection is disabled, you can configure a maximum of 63 policers per port (62 on every 4th port) for user-defined classes, and one for class-default for all switches. Any policy attachment or change that causes this limit to be exceeded fails with a *policer resources exceeded* error message.

- When CPU protection is disabled, you can configure a maximum of 255 policers on the ME3400E-24TS switch. Any policy attachment or change that causes this limit to be exceeded fails with a *policer resources exceeded* error message.
- If you disable CPU protection and attach a policy map with more than 45 policers, and then enable CPU protection again, and reload, 19 policers per port are again required for CPU protection. During reload, the policers 46 and above will reach the *policer resources exceeded* error condition and no policers are attached to those classes.

**Note**

For every four ports on a switch (port 1-4, 5-8, etc.), the first three ports support 64 policers, but the fourth port can support only 63 policers.

When you disable or enable the CPU protection feature, you must reload the switch by entering the **reload** privileged EXEC command before the configuration takes effect.

**Note**

When CPU protection is turned off, protocol packets can reach the CPU, which could cause CPU processing overload and storm control through software.

You can enter the **show policer cpu uni-eni {drop | rate}** privileged EXEC command to see if CPU protection is enabled.

For more information about control-plane security, see the software configuration guide for this release.

**Examples**

This example shows how to set CPU protection threshold to 10000 b/s and to verify the configuration.

```
Switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policer cpu uni 10000
Switch(config)# end
```

You can verify your settings by entering the **show policer cpu uni-eni rate** privileged EXEC command.

This example shows how to disable CPU protection and to reload the switch.

```
Switch(config)# no policer cpu uni all
Switch(config)# end
Switch# reload
Proceed with reload? [confirm]
```

This is an example of the output from the **show policer cpu uni-eni rate** privileged EXEC command when CPU protection is disabled:

```
Switch# show policer cpu uni-eni rate
CPU Protection feature is not enabled
```

**Related Commands\**

Command	Description
<a href="#">show policer cpu uni-eni rate</a>	Displays configured policer threshold for control-plane security.

# policy-map

Use the **policy-map** global configuration command to create or to modify a policy map that can be attached to multiple physical ports and to enter policy-map configuration mode. Use the **no** form of this command to delete an existing policy map.

**policy-map** *policy-map-name*

**no policy-map** *policy-map-name*

## Syntax Description

<i>policy-map-name</i>	Name of the policy map.
------------------------	-------------------------

## Defaults

No policy maps are defined. By default, packets are sent unmodified.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The switch supports a maximum of 256 unique policy maps.

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 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.

After entering the **policy-map** command, you enter policy-map configuration mode, and these configuration commands are available:

- **class**: the specified traffic classification for which the policy actions are applied. The classification is defined in the **class-map** global configuration command. For more information, see the [class-map](#) command.
- **description**: describes the policy map (up to 200 characters).
- **exit**: exits policy-map configuration mode and returns to global configuration mode.
- **no**: removes a previously defined policy map.



### Note

If you enter the **no** policy-map configuration command or the **no policy-map** *policy-map-name* global configuration command to delete a policy map that is attached to an interface, a warning message appears that lists any interfaces from which the policy map is being detached. The policy map is then detached and deleted. For example:

```
Warning: Detaching Policy test1 from Interface GigabitEthernet0/1
```

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 create input policy maps and output policy maps, and you can assign one input policy map and one output policy map to a port. The input policy map acts on incoming traffic on the port; the output policy map acts on outgoing traffic.

You can apply the same policy map to multiple physical ports.

Follow these guidelines when configuring input policy maps:

- The total number of input policy maps that can be attached to interfaces on the switch is limited by the availability of hardware resources. If you attempt to attach an input policy map that would exceed any hardware resource limitation, the configuration fails.
- An input policy map can contain a maximum of 64 class maps, plus **class-default**.
- You cannot configure an IP (IP standard and extended ACL, DSCP or IP precedence) and a non-IP (MAC ACL or CoS) classification within the same policy map, either within a single class map or across class maps within the policy map.
- After you use the **service-policy input** policy-map configuration command to attach an input policy map to an interface, you can modify the policy without detaching it from the interface. You can add or delete classification criteria, classes, or actions, or change the parameters of the configured actions (policers, rates, mapping, marking, and so on).
- These commands are not supported on input policy maps: **match qos-group** command, **bandwidth** command for Class-Based-Weighting-Queuing (CBWFQ), **priority** command for class-based priority queueing, **queue-limit** command for Weighted Tail Drop (WTD), **shape average** command for port shaping, or class-based traffic shaping.

Follow these guidelines when configuring output policy maps:

- Output policy maps can have a maximum of four classes, one of which is the **class-default**.
- The switch supports configuration and attachment of a unique output policy map for each port on the switch. However, these output policy maps can contain only three configurations of queue limits. You can include these three unique queue-limit configurations in as many output policy maps as there are switch ports. If you try to attach an output policy map that has a fourth queue-limit configuration, you see an error message, and the attachment is not allowed. There are no limitations on the configurations of bandwidth, priority, or shaping.
- All output policy maps must include the same number of class maps (one to three) and the same classification (that is, the same class maps).
- After you have attached a output policy map to an interface by using the **service-policy output** interface configuration command, you can only change the parameters of the configured actions (rates, percentages, and so on) or add or delete classification criteria of the class map while the policy map is attached to the interface. To add or delete a class or an action, you must detach the policy map from all interfaces, change it, and then reattach it to interfaces.
- These commands are not supported on output policy maps: **match access-group** command, **set** command for marking, and **police** command for policing without including the **priority** command.

For more information about policy maps, see the software configuration guide for this release.

**Examples**

This example shows how to create an input policy map for three classes:

```
Switch(config)# policy-map input-all
Switch(config-pmap)# class gold
Switch(config-pmap-c)# set dscp af43
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver
Switch(config-pmap-c)# police 50000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class bronze
Switch(config-pmap-c)# police 20000000
Switch(config-pmap-c)# exit
```

This example shows how to configure an output policy map that provides priority with rate limiting to the gold class and guarantees a minimum remaining bandwidth percent of 20 percent to the silver class and 10 percent to the bronze class:

```
Switch(config)# policy-map output-2
Switch(config-pmap)# class gold-out
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police 50000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver-out
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# class bronze-out
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
```

This example shows how to delete the policy map *output-2*:

```
Switch(config)# no policy-map output-2
```

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

**Related Commands**

Command	Description
<a href="#">class</a>	Defines a traffic classification match criteria for the specified class-map name.
<a href="#">class-map</a>	Creates a class map to be used for matching packets to the class whose name you specify.
<a href="#">service-policy (interface configuration)</a>	Applies a policy map to a port.
<a href="#">show policy-map</a>	Displays quality of service (QoS) policy maps.



# port-channel load-balance

Use the **port-channel load-balance** global configuration command to set the load-distribution method among the ports in the EtherChannel. Use the **no** form of this command to return to the default setting.

**port-channel load-balance { dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac }**

**no port-channel load-balance**

Syntax	Description
<b>dst-ip</b>	Load distribution is based on the destination host IP address.
<b>dst-mac</b>	Load distribution is based on the destination host MAC address. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel.
<b>src-dst-ip</b>	Load distribution is based on the source and destination host IP address.
<b>src-dst-mac</b>	Load distribution is based on the source and destination host MAC address.
<b>src-ip</b>	Load distribution is based on the source host IP address.
<b>src-mac</b>	Load distribution is based on the source MAC address. Packets from different hosts use different ports in the channel, but packets from the same host use the same port.

**Defaults** The default is **src-mac**.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** For information about when to use these forwarding methods, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

**Examples** This example shows how to set the load-distribution method to **dst-mac**:

```
Switch(config)# port-channel load-balance dst-mac
```

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

Related Commands	Command	Description
	<a href="#">interface port-channel</a>	Accesses or creates the port channel.
	<a href="#">show etherchannel</a>	Displays EtherChannel information for a channel.
	<a href="#">show running-config</a>	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: <a href="http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html">http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html</a> Select the <b>Cisco IOS Commands Master List, Release 12.2</b> to navigate to the command.

# port-type

Use the **port-type** interface configuration command to change the port type on a Cisco ME switch from its existing port type to a network node interface (NNI), a user network interface (UNI), or an enhanced network interfaces (ENI). Use the **no** form of this command to return the port to its default setting.

**port-type** { **eni** | **nni** | **uni** }

**no port-type**

## Syntax Description

<b>eni</b>	Enhanced network interface. ENIs have the same default configuration as UNIs, but you can configure ENI to support protocol control packets for Cisco Discovery Protocol (CDP), Spanning-Tree Protocol (STP), Link Layer Discovery Protocol (LLDP), and EtherChannel Link Aggregation Control Protocol (LACP) or Port Aggregation Protocol (PAgP).
<b>nni</b>	Network node interface.
<b>uni</b>	User network interface.

## Defaults

If no configuration file exists, all the 10/100 ports on the Cisco ME switch are UNIs, and the small form-factor pluggable (SFP) module slots on the Cisco ME switch are NNIs. You must configure a port to be an ENI port.

A port configured as an ENI has the same defaults as a UNI port, but the you can configure control protocols (CDP, STP, LLDP, LACP and PAgP) on ENIs. These protocols are not supported on UNIs.

The default status for a UNI or ENI is administratively down to prevent unauthorized users from gaining access to other ports as you configure the switch. You must use the **no shutdown** interface configuration command to enable a UNI or ENI before you can configure it.

The default status for an NNI is administratively up to allow a service provider remote access to the switch during initial configuration.

Configuring a port as an ENI does not change the administrative state of the port. If the port state is **shutdown** before a port-type change, it remains in **shutdown** state; if the state is **no shutdown**, it remains in **no shutdown** state.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

A port can be reconfigured to another port type. When a port is reconfigured as the other interface type, it inherits all the characteristics of that interface type. By default all ports on the switch are either UNI or NNI. At any time, all ports on the Cisco ME switch are UNIs, NNIs, or ENIs.

Some features are not supported only on all port types. Control protocols (CDP, STP, LLDP, and EtherChannel LACP and PAGP) have different support on each port type:

- On NNIs, these features are enabled by default.
- On ENIs, these features are disabled by default, but you can enable them by using the command-line interface.
- On UNIs, these features are not supported.

For information about specific feature support, see the software configuration guide for this release. When you change a port from one type to another, any features exclusive to a port type are removed from the configuration to prevent conflicting configuration options on a specific interface.

Every port on the switch can be a UNI or ENI, but when the switch is running the metro access image, only four ports can be NNIs at the same time. If the switch is running the metro IP access image, you can configure all ports as NNIs.

Entering the **no port-type** or **default port-type** interface configuration command returns the port to the default state: UNI for Fast Ethernet ports and NNI for Gigabit Ethernet ports.

Traffic is not switched between UNIs or ENIs, and all traffic incoming on UNIs or ENIs must exit on NNIs to prevent a user from gaining access to another user's private network. If it is appropriate for two or more UNIs or ENIs to exchange traffic within the switch, you can assign the interface to a community VLAN. A community VLAN can contain a maximum of eight UNIs or ENIs. We do not recommend mixing UNIs and ENIs in the same community VLAN.

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

## Examples

This example shows how to change a port to an NNI.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet0/1
Switch(config-if)# no shutdown
Switch(config-if)# port-type nni
5d20h: %SYS-5-CONFIG_I: Configured from console by console
Switch(config-if)# end
Switch# copy running-config startup-config
```

This example shows how to change a port type to an ENI.

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet0/1
Switch(config-if)# no shutdown
Switch(config-if)# port-type eni
Switch(config-if)# end
```

## Related Commands

Command	Description
<b>no shutdown</b>	Enables an interface.
<b>show interfaces</b>	Displays the statistical information specific to all interfaces or to a specific interface.
<b>show port-type</b>	Displays the port type of an interface.

## power-supply dual

Use the **power-supply dual** global configuration command to enable power-supply alarms (LED state, MIB state, and MIB traps) when only one power supply is installed in the switch. Use the **no** form of this command when running the switch on a single power supply to suppress the power-supply alarm for the missing second power supply. Use the **power-supply dual dc-feed** command to enable an alarm when a DC-power input is not present.

**power-supply dual [dc-feed]**

**no power-supply dual [dc-feed]**

<b>Syntax Description</b>	<b>dc-feed</b>	(Optional) Entering the <b>no power-supply dual dc-feed</b> command specifies that only one DC input is expected when a DC-power supply is installed. This suppresses any alarm associated with a missing DC input.
---------------------------	----------------	---

<b>Defaults</b>	The default is that no alarm occurs with only one installed power supply ( <b>no power-supply dual</b> ). The default when a DC-power supply is installed is that both DC inputs are providing power. If not, an alarm is triggered.
-----------------	--

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

<b>Usage Guidelines</b>	Entering the <b>no power-supply dual</b> global configuration command (the default) specifies that only one power supply is expected to be present. The switch does not generate an alarm when a power supply is missing.
-------------------------	---

This command controls only the sending of messages about the absence of a second power supply or the absence of input to the second power supply. The software detects whether a power supply is present and if there is an input voltage. When there is input, the software can detect if there is an output voltage and if the fan is operating.

- If only one power supply is present, no alarm is sent. However, if this power supply is connected to the AC input and is not receiving or sending power, a power-supply fault message is sent.
- If two power supplies are present, and both are receiving and sending power, no message is sent.
- If two power supplies are present, and one is connected and operating and the other is not connected to the AC input, no message is sent.
- If two power supplies are present and both are connected to AC inputs, but only one is receiving or sending power, a power-supply fault message is sent.

**Note**

The switch always sends an error message when an AC-power supply is connected to an AC input but is not receiving or sending power.

If you operate the switch with two power supplies, enter the **power-supply dual** global configuration command to configure the switch to send a message when one power supply is missing.

When one or two DC-power supplies are installed, if the switch does not detect both DC inputs, it creates an LED alarm color and sends a system message. If you want to use only one DC input, enter the **no power-supply dual dc-feed** global configuration command to disable alarm messages if the second DC input is not present. This command is valid only when DC-power supplies are installed in the switch.

**Examples**

This example shows how to suppress power-supply alarms for a missing second power supply and to verify the configuration:

```
Switch(config)# no power-supply dual
Switch(config)# end
Switch# show env power
POWER SUPPLY 1 is DC OK
  DC A Input: OK
  DC B Input: OK
  Output      : OK
  Fan         : OK
POWER SUPPLY 2 is DC OK
  DC A Input: OK
  DC B Input: OK
  Output      : OK
  Fan         : OK
```

This example shows how to suppress power-supply alarms when a DC-power supply is installed and only one DC input is present:

```
Switch(config)# no power-supply dual dc-feed
Switch(config)# end
```

You can display the power-supply alarm status by entering the **show env all** or **show env power** privileged EXEC commands.

**Related Commands**

Command	Description
<b>show env {all   power}</b>	Displays the power-supply alarm setting for the switch.

# priority

Use the **priority** policy-map class configuration command to configure class-based priority queuing for a class of traffic belonging to an output policy map. The switch supports strict priority queuing or priority used with the **police** policy-map command. Use the **no** form of this command to remove a priority specified for a class.

**priority**

**no priority**



## Note

When the **police** command is used with the **priority** policy-map class command for unconditionally rate-limiting the priority queue, burst size values are not supported for the **police** command.

## Syntax Description

This command has no arguments or keywords.

## Defaults

No policers are defined.

## Command Modes

Policy-map class configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

When used by itself (not followed by the **police** policy-map command), the **priority** command assigns traffic to a low-latency path and ensures that packets belonging to the class have the lowest possible latency. With strict priority queuing, packets in the priority queue are scheduled and sent until the queue is empty.



## Note

You should exercise care when using the **priority** command without the **police** command. Excessive use of strict priority queuing might cause congestion in other queues.

You can use **priority** with the **police** *{rate-bps | cir cir-bps}* policy-map command to reduce the bandwidth used by the priority queue. This is the only form of policing that is supported in output policy maps. Using this combination of commands configures a maximum rate on the priority queue and allows you to use the **bandwidth** and **shape average** policy-map commands for other classes to allocate traffic rates on other queues.



## Note

When you use the **police** command with the **priority** command in an output policy, the police rate range is 64000 to 1000000000 bps, even though the range that appears in the command-line help is 8000 to 1000000000. Configured burst size is ignored when you try to attach the output service policy.

When you configure priority in an output policy map without the **police** command, you can only configure the other queues for sharing by using the **bandwidth remaining percent** policy-map class command. This command does not guarantee the allocated bandwidth, but the rate of distribution.

When you configure priority in an output policy map with the **police** command, you can configure other queues for sharing by using the **bandwidth** policy-map class command and for shaping by using the **shape average** policy-map class command.

You can associate the **priority** command only with a single unique class for all attached output policies on the switch.

You cannot associate the **priority** command with the **class-default** of the output policy map.

You cannot configure priority and any other scheduling action (**shape average** or **bandwidth**) in the same class.

The **priority** command uses a default queue limit for the class. You can change the queue limit by using the **queue-limit** policy-map class command, overriding the default set by the **priority** command.

## Examples

This example shows how to configure the class *out-class1* as a strict priority queue so that all packets in that class are sent before any other class of traffic. Other traffic queues are configured so that *out-class-2* gets 50 percent of the remaining bandwidth and *out-class3* gets 20 percent of the remaining bandwidth. The class **class-default** receives the remaining 30 percent with no guarantees.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# exit
```

This example shows how to use the **priority** with **police** commands to configure *out-class1* as the priority queue, with traffic going to the queue limited to 20000000 bits per second (bps) so that the priority queue never uses more than that. Traffic above that rate is dropped. The other traffic queues are configured as in the previous example.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police 20000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# exit
```

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



Related Commands	Command	Description
	<a href="#">class</a>	Defines a traffic classification match criteria for the specified class-map name.
	<a href="#">police</a>	Defines a policer for classified traffic.
	<a href="#">policy-map</a>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
	<a href="#">show policy-map</a>	Displays quality of service (QoS) policy maps.

## private-vlan

Use the **private-vlan** VLAN configuration command to configure private VLANs and to configure the association between private-VLAN primary and secondary VLANs. Use the **no** form of this command to return the VLAN to normal VLAN configuration.

**private-vlan** { **association** [**add** | **remove**] *secondary-vlan-list* | **community** | **isolated** | **primary** }

**no private-vlan** { **association** | **community** | **isolated** | **primary** }

### Syntax Description

<b>association</b>	Create an association between the primary VLAN and a secondary VLAN.
<i>secondary-vlan-list</i>	Specify one or more secondary VLANs to be associated with a primary VLAN in a private VLAN.
<b>add</b>	Associate a secondary VLAN to a primary VLAN.
<b>remove</b>	Clear the association between a secondary VLAN and a primary VLAN.
<b>community</b>	Designate the VLAN as a community VLAN.
<b>isolated</b>	Designate the VLAN as a community VLAN.
<b>primary</b>	Designate the VLAN as a community VLAN.

### Defaults

The default is to no configured private VLANs.

### Command Modes

VLAN configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

You must manually configure private VLANs on all switches in the Layer 2 network to merge their Layer 2 databases and to prevent flooding of private-VLAN traffic.

You cannot include VLAN 1 or VLANs 1002 to 1005 in the private-VLAN configuration. Extended VLANs (VLAN IDs 1006 to 4094) can be configured as private VLANs.

You can **associate** a secondary (isolated or community) VLAN with only one primary VLAN. A primary VLAN can have one isolated VLAN and multiple community VLANs associated with it.

- A secondary VLAN cannot be configured as a primary VLAN.
- The *secondary\_vlan\_list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private-VLAN ID or a hyphenated range of private-VLAN IDs. The list can contain one isolated VLAN and multiple community VLANs.
- If you delete either the primary or secondary VLANs, the ports associated with the VLAN become inactive.

A **community** VLAN carries traffic among community ports and from community ports to the promiscuous ports on the corresponding primary VLAN. A community VLAN can include no more than eight user network interfaces (UNIs).

An **isolated** VLAN is used by isolated ports to communicate with promiscuous ports. It does not carry traffic to other community ports or to isolated ports with the same primary VLAN domain.

A **primary** VLAN is the VLAN that carries traffic from a gateway to customer end stations on private ports.

Configure Layer 3 VLAN interfaces (SVIs) only for primary VLANs. You cannot configure Layer 3 VLAN interfaces for secondary VLANs. SVIs for secondary VLANs are inactive while the VLAN is configured as a secondary VLAN.

The **private-vlan** commands do not take effect until you exit from VLAN configuration mode.

Do not configure private-VLAN ports as EtherChannels. While a port is part of the private-VLAN configuration, any EtherChannel configuration for it is inactive.

A private VLAN cannot be a Remote Switched Port Analyzer (RSPAN) VLAN.

A private VLAN cannot be a user network interface-enhanced network interface (UNI-ENI) VLAN. If the VLAN is a UNI-ENI isolated VLAN (the default), you can change it to a private VLAN by entering the **private-vlan** VLAN configuration command. If a VLAN has been configured as a UNI-ENI community VLAN, you must first enter the **no uni-vlan** VLAN configuration command before configuring it as a private VLAN.

Although a private VLAN contains more than one VLAN, only one STP instance runs for the entire private VLAN. When a secondary VLAN is associated with the primary VLAN, the STP parameters of the primary VLAN are propagated to the secondary VLAN.

See the [switchport private-vlan](#) command for information about configuring host ports and promiscuous ports.



#### Note

For more information about private-VLAN interaction with other features, see the software configuration guide for this release.

#### Examples

This example shows how to configure VLAN 20 as a primary VLAN, VLAN 501 as an isolated VLAN, VLANs 502 and 503 as community VLANs, and to associate them in a private VLAN. The example assumes that VLANs 502 and 503 were previously configured as UNI-ENI community VLANs.

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 501
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 502
Switch(config-vlan)# no uni-vlan
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 503
Switch(config-vlan)# no uni-vlan
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan association 501-503
Switch(config-vlan)# end
```

You can verify your setting by entering the **show vlan private-vlan** or **show interfaces status** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">show interfaces status</a>	Displays the status of interfaces, including the VLANs to which they belong.
	<a href="#">show vlan private-vlan</a>	Displays the private VLANs and VLAN associations configured on the switch.
	<a href="#">switchport private-vlan</a>	Configures a private-VLAN port as a host port or promiscuous port.

## private-vlan mapping

Use the **private-vlan mapping** interface configuration command on a switch virtual interface (SVI) to create a mapping between a private-VLAN primary and secondary VLANs so that both VLANs share the same primary VLAN interface. Use the **no** form of this command to remove private-VLAN mappings from the interface.

**private-vlan mapping** {[add | remove] *secondary-vlan-list*}

**no private-vlan mapping**

Syntax Description	<i>secondary-vlan-list</i>	Specify one or more secondary VLANs to be mapped to the primary VLAN interface.
<b>add</b>		(Optional) Map the secondary VLAN to the primary VLAN interface.
<b>remove</b>		(Optional) Remove the mapping between the secondary VLAN and the primary VLAN interface.

**Defaults** The default is to have no private VLAN mapping configured.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines**

The SVI of the primary VLAN is created at Layer 3.

Configure Layer 3 VLAN interfaces (SVIs) only for primary VLANs. You cannot configure Layer 3 VLAN interfaces for secondary VLANs. SVIs for secondary VLANs are inactive while the VLAN is configured as a secondary VLAN.

The *secondary\_vlan\_list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private-VLAN ID or a hyphenated range of private-VLAN IDs. The list can contain one isolated VLAN and multiple community VLANs.

Traffic that is received on the secondary VLAN is routed by the interface of the primary VLAN.

A secondary VLAN can be mapped to only one primary VLAN. IF you configure the primary VLAN as a secondary VLAN, all SVIs specified in this command are brought down.

If you configure a mapping between two VLANs that do not have a valid Layer 2 private-VLAN association, the mapping configuration does not take effect.

**Examples**

This example shows how to map the interface of VLAN 20 to the SVI of VLAN 18:

```
Switch# configure terminal
Switch# interface vlan 18
Switch(config-if)# private-vlan mapping 20
Switch(config-vlan)# end
```

This example shows how to permit routing of secondary VLAN traffic from secondary VLANs 303 to 305 and 307 through VLAN 20 SVI:

```
Switch# configure terminal
Switch# interface vlan 20
Switch(config-if)# private-vlan mapping 303-305, 307
Switch(config-vlan)# end
```

You can verify your setting by entering the **show interfaces private-vlan mapping** privileged EXEC command.

**Related Commands**

Command	Description
<a href="#">show interfaces private-vlan mapping</a>	Display private-VLAN mapping information for interfaces or VLAN SVIs.

# queue-limit

Use the **queue-limit** policy-map class configuration command to set the queue maximum threshold for weighted tail drop (WTD) in an output policy map. Use the **no** form of this command to return to the default.

**queue-limit** [*cos value* | **dot1ad dei** *value* | **dscp** *value* | **precedence** *value* | **qos-group** *value*]  
*number-of-packets* [**packets**]

**no queue-limit** [*cos value* | **dot1ad dei** *value* | **dscp** *value* | **precedence** *value* | **qos-group** *value*]  
*number-of-packets* [**packets**]

## Syntax Description

<i>cos value</i>	(Optional) Set the parameters for each cost of service (CoS) value. The range is from 0 to 7.
<b>dot1ad dei</b> <i>value</i>	(Optional) Set the parameters for each drop eligibility indicator (DEI) value. The range is from 0 to 1.
<b>dscp</b> <i>value</i>	(Optional) Set the parameters for each Differentiated Services Code Point (DSCP) value. The range is from 0 to 63.
<b>precedence</b> <i>value</i>	(Optional) Set the parameters for each IP precedence value. The range is from 0 to 7.
<b>qos-group</b> <i>value</i>	(Optional) Set the parameters for each quality-of-service (QoS) group value. The range is from 0 to 99.
<i>number-of-packets</i> [ <b>packets</b> ]	Set the maximum threshold for WTD as the number of packets in the queue. The range is from 16 to 544 and refers to 256-byte packets. The default is 160 packets. The <b>packets</b> keyword is optional.
	<b>Note</b> For optimal network performance, we strongly recommend that you configure the maximum queue-limit to 272 or less.

## Defaults

Default queue limit is 160 (256-byte) packets.

## Command Modes

Policy-map class configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.
12.2(55)SE	The <b>dot1ad dei</b> keywords were added.

## Usage Guidelines

You use the **queue-limit** policy-map class command to control output traffic. Queue-limit settings are not supported in input policy maps.

Beginning with Cisco IOS Release 12.2(35)SE, the switch supports one output policy map for each interface. However, the limit of three unique queue-limit configurations across all output policy maps remains in effect. You can use the same queue-limit configuration across multiple policy maps.

Within an output policy map only four queues (classes) are allowed, including the class default. Each queue has three defined thresholds (queue limits). Only three queue-limit configurations are allowed on the switch, but multiple policy maps can share the same queue-limits. For two policy maps to share a queue-limit configuration, all threshold values must be the same for all classes in both policy maps.

If you try to attach an output policy map that contains a fourth queue-limit configuration to an interface, you see an error message, and the attachment is not allowed.

The **queue-limit** command is supported only after you first configure a scheduling action, such as **bandwidth**, **shape-average**, or **priority**, except when you configure **queue-limit** in the **class-default** of an output policy map.

You cannot configure more than two unique threshold values for WTD qualifiers (**cos**, **dscp**, **precedence**, or **qos-group**) in the **queue-limit** command. However, you can map any number of qualifiers to those thresholds. You can configure a third unique threshold value to set the maximum queue, using the **queue-limit** command with no qualifiers.

When you use the **queue-limit** command to configure thresholds within a class map, the WTD thresholds must be less than or equal to the maximum threshold of the queue. This means that the queue size configured without a qualifier must be larger than any of the queue sizes configured with a qualifier.

## Examples

This example shows how to configure WTD so that *out-class1*, *out-class2*, *out-class3*, and **class-default** get a minimum of 40, 20, 10 and 10 percent of the traffic bandwidth respectively. The corresponding queue-sizes are set to 48, 32, 16 and 272 (256-byte) packets:

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# bandwidth percent 40
Switch(config-pmap-c)# queue-limit 48
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# queue-limit 32
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit 16
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit 272
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```



This example shows how to configure WTD for a Fast Ethernet port where *outclass1*, *outclass2*, and *outclass3* get a minimum of 50, 20, and 10 percent of the traffic bandwidth. The **class-default** gets the remaining 20 percent. Each corresponding queue size is set to 64, 32, and 16 (256-byte) packets, respectively. The example also shows how if *outclass1* matches to dscp 46, 56, 57, 58, 60, 63, a DSCP value of 46 gets a queue size of 32 (256-byte) packets; DSCP values 56, 57, and 58 get queue sizes of 48 (256-byte) packets; and the remaining DSCP values of 60 and 63 get the default queue size of 64 (256-byte) packets.

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# queue-limit 64
Switch(config-pmap-c)# queue-limit dscp 46 32
Switch(config-pmap-c)# queue-limit dscp 56 48
Switch(config-pmap-c)# queue-limit dscp 57 48
Switch(config-pmap-c)# queue-limit dscp 58 48
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# queue-limit 32
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit 16
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

You can use these same queue-limit values in multiple output policy maps on the switch. However, changing one of the queue-limit values in a class would create a new, unique queue-limit configuration. You can attach only three unique queue-limit configurations in output policy maps to interfaces at any one time. If you try to attach an output policy map with a fourth unique queue-limit configuration, you see this error message:

```
QoS: Configuration failed. Maximum number of allowable unique queue-limit
configurations exceeded.
```

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

Related Commands	Command	Description
	<b>class</b>	Defines a traffic classification match criteria for the specified class-map name.
	<b>policy-map</b>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
	<b>show policy-map</b>	Displays QoS policy maps.

## remote-span

Use the **remote-span** VLAN configuration command to configure a VLAN as a Remote Switched Port Analyzer (RSPAN) VLAN. Use the **no** form of this command to remove the RSPAN designation from the VLAN.

**remote-span**

**no remote-span**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No RSPAN VLANs are defined.

**Command Modes** VLAN configuration (config-VLAN)

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

Valid RSPAN VLAN IDs are 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).

Before you configure the RSPAN **remote-span** command, use the **vlan** global configuration command to create the VLAN.

- To change a VLAN from a user network interface-enhanced network interface (UNI-ENI) isolated VLAN (the default) to an RSPAN VLAN, enter the **rspan-vlan** VLAN configuration command.
- To change a UNI-ENI community VLAN to an RSPAN VLAN, you must first remove the community VLAN type by entering the **no uni-vlan** VLAN configuration command.

The RSPAN VLAN has these characteristics:

- No MAC address learning occurs on it.
- RSPAN VLAN traffic flows only on trunk ports.
- Spanning Tree Protocol (STP) can run in the RSPAN VLAN, but it does not run on RSPAN destination ports. On the Cisco ME switch only network node interfaces (NNIs) or enhanced network interfaces (ENIs) on which STP has been enabled participate in STP.

You must manually also configure both source, destination, and intermediate switches (those in the RSPAN VLAN between the source switch and the destination switch) with the RSPAN VLAN ID.

When an existing VLAN is configured as an RSPAN VLAN, the VLAN is first deleted and then recreated as an RSPAN VLAN. Any access ports become inactive until the RSPAN feature is disabled.

---

**Examples**

This example shows how to configure a VLAN as an RSPAN VLAN.

```
Switch(config)# vlan 901  
Switch(config-vlan)# remote-span
```

This example shows how to remove the RSPAN feature from a VLAN.

```
Switch(config)# vlan 901  
Switch(config-vlan)# no remote-span
```

You can verify your settings by entering the **show vlan remote-span** user EXEC command.

---

**Related Commands**

Command	Description
<a href="#">monitor session</a>	Enables Switched Port Analyzer (SPAN) and RSPAN monitoring on a port and configures a port as a source or destination port.
<a href="#">vlan</a>	Changes to config-vlan mode where you can configure VLANs 1 to 4094.

# renew ip dhcp snooping database

Use the **renew ip dhcp snooping database** privileged EXEC command to renew the DHCP snooping binding database.

```
renew ip dhcp snooping database [validation none] [{flash:/filename |
ftp://user:password@host/filename | nvram:/filename | rcp://user@host/filename |
tftp://host/filename}] [validation none]
```

Syntax Description		
<b>validation none</b>	(Optional) Specify that the switch does not verify the cyclic redundancy check (CRC) for the entries in the binding file specified by the URL.	
<b>flash:/filename</b>	(Optional) Specify that the database agent or the binding file is in the flash memory.	
<b>ftp://user:password@host/filename</b>	(Optional) Specify that the database agent or the binding file is on an FTP server.	
<b>nvram:/filename</b>	(Optional) Specify that the database agent or the binding file is in the NVRAM.	
<b>rcp://user@host/filename</b>	(Optional) Specify that the database agent or the binding file is on a Remote Control Protocol (RCP) server.	
<b>tftp://host/filename</b>	(Optional) Specify that the database agent or the binding file is on a TFTP server.	

**Defaults** No default is defined.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** If you do not specify a URL, the switch tries to read the file from the configured URL.

**Examples** This example shows how to renew the DHCP snooping binding database without checking CRC values:

```
Switch# renew ip dhcp snooping database validation none
```

You can verify settings by entering the **show ip dhcp snooping database** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">ip dhcp snooping</a>	Enables DHCP snooping on a VLAN.
	<a href="#">ip dhcp snooping binding</a>	Configures the DHCP snooping binding database.
	<a href="#">show ip dhcp snooping database</a>	Displays the status of the DHCP snooping database agent.

# rep admin vlan

Use the **rep admin vlan** global configuration command to configure a Resilient Ethernet Protocol (REP) administrative VLAN for REP to transmit hardware flood layer (HFL) messages. Use the **no** form of this command to return to the default configuration with VLAN 1 as the administrative VLAN.

```
rep admin vlan vlan-id
```

```
no rep admin vlan
```

## Syntax Description

<i>vlan-id</i>	The VLAN ID range is from 1 to 4094. The default is VLAN 1; the range to configure is 2 to 4094.
----------------	--

## Defaults

The administrative VLAN is VLAN 1.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

If the VLAN does not already exist, this command does not create the VLAN.

To avoid the delay introduced by relaying messages in software for link-failure or VLAN-blocking notification during load balancing, REP floods packets at the hardware flood layer (HFL) to a regular multicast address. These messages are flooded to the whole network, not just the REP segment. Switches that do not belong to the segment treat them as data traffic. Configuring an administrative VLAN for the whole domain can control flooding of these messages.

If no REP administrative VLAN is configured, the default is VLAN 1.

There can be only one administrative VLAN on a switch and on a segment.

The administrative VLAN cannot be the RSPAN VLAN.

## Examples

This example shows how to configure VLAN 100 as the REP administrative VLAN:

```
Switch (config)# rep admin vlan 100
```

You can verify your settings by entering the **show interface rep detail** privileged EXEC command.

## Related Commands

Command	Description
<a href="#">show interfaces rep detail</a>	Displays detailed REP configuration and status for all interfaces or the specified interface, including the administrative VLAN.

## rep block port

Use the **rep block port** interface configuration command on the REP primary edge port to configure Resilient Ethernet Protocol (REP) VLAN load balancing. Use the **no** form of this command to return to the default configuration.

```
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

<b>id</b> <i>port-id</i>	Identify the VLAN blocking alternate port by entering the unique port ID that is automatically generated when REP is enabled. The REP port ID is a 16-character hexadecimal value. You can view the port ID for an interface by entering the <b>show interface interface-id rep detail</b> command.
<i>neighbor_offset</i>	Identify the VLAN blocking alternate port by entering the offset number of a neighbor. The range is -256 to +256; a value of 0 is invalid. 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.
<b>preferred</b>	Identify the VLAN blocking alternate port as the segment port on which you entered the <b>rep segment segment-id preferred</b> interface configuration command. <b>Note</b> Entering the <b>preferred</b> keyword does not ensure that the preferred port is the alternate port; it gives it preference over other similar ports.
<b>vlan</b>	Identify the VLANs to be blocked.
<i>vlan-list</i>	Enter a VLAN ID from 1 to 4094 or a range or sequence of VLANs (such as 1-3, 22, 41-44) of VLANs to be blocked.
<b>all</b>	Enter to block all VLANs.

### Defaults

The default behavior after you enter the **rep preempt segment** privileged EXEC command (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

### Command History

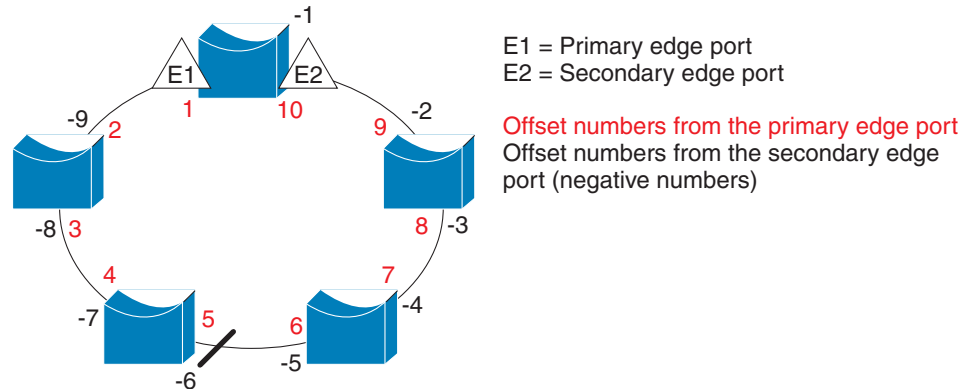
Release	Modification
12.2(44)EY	This command was introduced.

### 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. See [Neighbor Offset Numbers in a REP Segment](#) Figure 2-1.

**Figure 2-1 Neighbor Offset Numbers in a REP Segment**



201890

**Note**

You would never 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** interface configuration command 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. The port ID format is similar to the one used by the spanning tree algorithm: a port number (unique on the bridge) associated to a MAC address (unique in the network). To determine the port ID of a port, enter the **show interface interface-id rep detail** privileged EXEC command.

There is no limit to the number of times that you can enter the **rep block port id port-id vlan vlan-list** interface configuration command. You can block an unlimited number, range, or sequence of VLANs.

When you use the **rep block port id port-id vlan vlan-list** interface configuration command on a REP primary edge port to block a VLAN list and then use the same command to block another VLAN list on the same port, the second VLAN list does not replace the first VLAN list but is appended to the first VLAN list.

When you use the **rep block port id port-id vlan vlan-list** interface configuration command on a REP primary edge port to block a VLAN list on one port and then use the same command to block another VLAN list on another port, the original port number and VLAN list are overwritten.

**Examples**

This example shows how to configure REP VLAN load balancing on the Switch B primary edge port (Gigabit Ethernet port 0/1) and to configure Gigabit Ethernet port 0/2 of Switch A as the alternate port to block VLANs 1 to 100. The alternate port is identified by its port ID, shown in bold in the output of the **show interface rep detail** command for the Switch A port.

```
Switch A# show interface gigabitethernet0/2 rep detail
```

```
GigabitEthernet0/2 REP enabled
Segment-id: 2 (Segment)
PortID: 0080001647FB1780
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 007F001647FB17800EEE
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 1
Preempt Delay Timer: 35 sec
Load-balancing block port: none
Load-balancing block vlan: none
STCN Propagate to:
PDU/TLV statistics:
LSL PDU rx: 107122, tx: 192493
```

```
Switch B# config t
```

```
Switch (config)# interface gigabitethernet0/1
Switch (config-if)# rep block port id 0080001647FB1780 vlan 1-100
Switch (config-if)# exit
```

This example shows how to configure VLAN load balancing by using a neighbor offset number and how to verify the configuration by entering the **show interfaces rep detail** privileged EXEC command:

```
Switch# config t
```

```
Switch (config)# interface gigabitethernet0/2
Switch (config-if)# rep block port 6 vlan 1-110
Switch (config-if)# end
```

```
Switch# show interface gigabitethernet0/2 rep detail
```

```
GigabitEthernet0/2 REP enabled
Segment-id: 2 (Segment)
PortID: 0080001647FB1780
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 007F001647FB178009C3
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 3
Preempt Delay Timer: 35 sec
Load-balancing block port: 6
Load-balancing block vlan: 1-110
STCN Propagate to: none
LSL PDU rx: 1466780, tx: 3056637
HFL PDU rx: 2, tx: 0
BPA TLV rx: 1, tx: 2119695
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 757406, tx: 757400
EPA-COMMAND TLV rx: 1, tx: 1
EPA-INFO TLV rx: 178326, tx: 178323
```

## Related Commands

Command	Description
<a href="#">rep preempt delay</a>	Configures a waiting period after a segment port failure and recovery before REP VLAN load balancing is triggered.



Command	Description
<a href="#">rep preempt segment</a>	Manually starts REP VLAN load balancing on a segment.
<a href="#">show interfaces rep detail</a>	Displays REP detailed configuration and status for all interfaces or the specified interface, including the administrative VLAN.

## rep lsl-age-timer

Use the **rep lsl-age-timer** interface configuration command on a Resilient Ethernet Protocol (REP) port to configure the Link Status Layer (LSL) age timer for the time period that the REP interface remains up without receiving a hello from the REP neighbor. Use the **no** form of this command to return to the default time.

**rep lsl-age timer** *value*

**no rep lsl-age timer**

<b>Syntax Description</b>	<i>value</i>	The age-out time in milliseconds. The range is from 120 to 10000 ms in 40-ms increments. The default is 5000 ms (5 seconds).
---------------------------	--------------	--

<b>Defaults</b>	The REP link shuts down if it does not receive a hello message from a neighbor for 5000 ms.
-----------------	---

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(50)SE	This command was introduced.
	12.2(52)SE	The age-out timer interval range changed to 120 to 10000 ms in 40-ms increments.

<b>Usage Guidelines</b>	<p>The LSL hello timer is set to the age-timer value divided by 3 so that there should be at least two LSL hellos sent during the LSL age timer period. If no hellos are received within that time, the REP link shuts down.</p>
-------------------------	--

In Cisco IOS Release 12.2(52)SE, the LSL age-timer range changed from 3000 to 10000 ms in 500-ms increments to 120 to 10000 ms in 40-ms increments. If the REP neighbor device is not running Cisco IOS Release 12.2(52)SE or later, you must use the shorter time range because the device does not accept values out of the earlier range.

EtherChannel port channel interfaces do not support LSL age-timer values less than 1000 ms. If you try to configure a value less than 1000 ms on a port channel, you receive an error message and the command is rejected.

<b>Examples</b>	This example shows how to configure the REP LSL age timer on a REP link to 7000 ms:
-----------------	---

```
Switch (config)# interface gigabitethernet0/2
Switch (config-if)# rep lsl-age-timer 7000
Switch (config-if)# exit
```

You can verify the configured ageout time by entering the **show interfaces rep detail** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">show interfaces rep</a> [detail]	Displays REP configuration and status for all interfaces or the specified interface, including the configured LSL age-out timer value.

## rep preempt delay

Use the **rep preempt delay** interface configuration command on the REP primary edge port to configure a waiting period after a segment port failure and recovery before Resilient Ethernet Protocol (REP) VLAN load balancing is triggered. Use the **no** form of this command to remove the configured delay.

**rep preempt delay** *seconds*

**no rep preempt delay**

### Syntax Description

*seconds* Set the number of seconds to delay REP preemption. The range is 15 to 300.

### Defaults

No preemption delay is set. If you do not enter the **rep preempt delay** command, the default is manual preemption with no delay.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(44)EY	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 if you want 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 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.

### Examples

This example shows how to configure a REP preemption time delay of 100 seconds on the primary edge port:

```
Switch (config)# interface gigabitethernet0/1
Switch (config-if)# rep preempt delay 100
Switch (config-if)# exit
```

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

Related Commands	Command	Description
	<a href="#">rep block port</a>	Configures VLAN load balancing.
	<a href="#">show interfaces rep</a>	Displays REP configuration and status for all interfaces or a specified interface.

# rep preempt segment

Use the **rep preempt segment** privileged EXEC command to manually start Resilient Ethernet Protocol (REP) VLAN load balancing on a segment.

**rep preempt segment** *segment-id*

## Syntax Description

<i>segment-id</i>	ID of the REP segment. The range is from 1 to 1024.
-------------------	---

## Defaults

Manual preemption is the default behavior.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

When you enter the **rep preempt segment** *segment-id* command, a confirmation message appears before the command is executed because preemption can cause network disruption.

Enter this command on the switch on the segment that has 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** **{id port-id | neighbor\_offset | preferred} vlan {vlan-list | all}** interface configuration command on the REP primary edge port before you manually start preemption.

There is not a **no** version of this command.

## Examples

This example shows how to manually trigger REP preemption on segment 100 with the confirmation message:

```
Switch)# rep preempt segment 100
The command will cause a momentary traffic disruption.
Do you still want to continue? [confirm]
```

## Related Commands

Command	Description
<a href="#">rep block port</a>	Configures VLAN load balancing.
<a href="#">show interfaces rep</a> [ <b>detail</b> ]	Displays REP configuration and status for all interfaces or the specified interface.

# rep segment

Use the **rep segment** interface configuration command to enable Resilient Ethernet Protocol (REP) on the interface and to assign a segment ID to it. Use the **no** form of this command to disable REP on the interface.

**rep segment** *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**]

**no rep segment**

## Syntax Description

<i>segment-id</i>	Assign a segment ID to the interface. The range is from 1 to 1024.
<b>edge</b>	(Optional) Identify the interface as one of the two REP edge ports. Entering the <b>edge</b> keyword without the <b>primary</b> keyword configures the port as the secondary edge port.
<b>no-neighbor</b>	(Optional) Configure a segment edge with no external REP neighbor.
<b>primary</b>	(Optional) On an edge port, specify that the port is the primary edge port. A segment has only one primary edge port. If you configure two ports in a segment as the primary edge port, for example ports on different switches, the REP selects one of them to serve as the segment primary edge port.
<b>preferred</b>	(Optional) Specify that the port is the preferred alternate port or the preferred port for VLAN load balancing.
<b>Note</b>	Configuring a port as preferred 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.

## Defaults

REP is disabled on the interface.

When REP is enabled on an interface, the default is for the port to be a regular segment port.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.
12.2(50)SE	The <b>no-neighbor</b> keyword was added.

## Usage Guidelines

REP ports must be Layer 2 trunk ports.

A non-ES REP port can be either an IEEE 802.1Q trunk port or an ISL trunk port.

REP ports should not be configured as one of these port types:

- SPAN destination port
- Private VLAN port
- Tunnel port

- Access port
- REP ports must be network node interfaces (NNIs). REP ports cannot be user-network interfaces (UNIs) or enhanced network interfaces (ENIs).

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 you configure two ports in a segment as the primary edge port, for example ports on different switches, the configuration is allowed, but the REP selects one of them to serve as the segment primary edge port.

- REP ports follow these rules:
  - There is no limit to the number of REP ports on a switch; however, only two ports on a switch can belong to the same REP segment.
  - If only one port on a switch is configured in a segment, the port should be an edge port.
  - If two ports on a switch belong to the same segment, they must be both edge ports, both regular segment ports, or one regular port and one edge no-neighbor port. An edge port and regular segment port on a switch cannot belong to the same segment.
  - If two ports on a switch 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.

If you configure two ports in a segment as the primary edge port, for example ports on different switches, the REP selects one of them to serve as the segment primary edge port. Enter the **show rep topology** privileged EXEC command on a port in the segment to verify which port is the segment primary edge port.

REP interfaces come up in a blocked state and remain in a blocked state until notified that it is safe to unblock. You need to be aware of this to avoid sudden connection losses.

You should configure REP only in networks with redundancy. Configuring REP in a network without redundancy causes loss of connectivity.

In networks where ports on a neighboring switch do not support REP, you can configure the non-REP facing ports as edge no-neighbor ports. These ports inherit all properties of edge ports and you can configure them as any other edge port, including to send STP or REP topology change notices to the aggregation switch. In this case, the STP topology change notice (TCN) that is sent is a multiple spanning-tree (MST) STP message.

## Examples

This example shows how to enable REP on a regular (nonedge) segment port:

```
Switch (config)# interface gigabitethernet0/1
Switch (config-if)# rep segment 100
```

This example shows how to enable REP on a port and to identify the port as the REP primary edge port:

```
Switch (config)# interface gigabitethernet0/2
Switch (config-if)# rep segment 100 edge primary
```

This example shows how to configure the same configuration when the interface has no external REP neighbor:

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet0/1
Switch (conf-if)# rep segment 100 edge no-neighbor primary
```

This example shows how to enable REP on a port and to identify the port as the REP secondary edge port:

```
Switch (config)# interface gigabitethernet0/2
```



```
Switch (config-if)# rep segment 100 edge
```

You can verify your settings by entering the **show interfaces rep** privileged EXEC command. To verify which port in the segment is the primary edge port, enter the **show rep topology** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">show interfaces rep</a> [detail]	Displays REP configuration and status for all interfaces or the specified interface.
	<a href="#">show rep topology</a> [detail]	Displays information about all ports in the segment, including which one was configured and selected as the primary edge port.

# rep stcn

Use the **rep stcn** interface configuration command on a Resilient Ethernet Protocol (REP) edge port to configure the port to send REP segment topology change notifications (STCNs) to another interface, to other segments, or to Spanning Tree Protocol (STP) networks. Use the **no** form of this command to disable the sending of STCNs to the interface, segment, or STP network.

```
rep stcn {interface interface-id | segment id-list | stp}
```

```
no rep stcn {interface | segment | stp}
```

## Syntax Description

<b>interface</b> <i>interface-id</i>	Identify a physical interface or port channel to receive STCNs.
<b>segment</b> <i>id-list</i>	Identify one REP segment or list of segments to receive STCNs. The range is 1 to 1024. You can also configure a sequence of segments (for example 3-5, 77, 100).
<b>stp</b>	Send STCNs to an STP network.

## Defaults

Transmission of STCNs to other interfaces, segments, or STP networks is disabled.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

Enter this command on a segment edge port.

You use this command to notify other portions of the Layer 2 network of topology changes that occur in the local REP segment. This removes obsolete entries in the Layer 2 forwarding table in other parts of the network, which allows faster network convergence.

## Examples

This example shows how to configure the REP primary edge port to send STCNs to segments 25 to 50:

```
Switch (config)# interface gigabitethernet0/2
Switch (config-if)# rep stcn segment 25-50
Switch (config-if)# exit
```

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

## Related Commands

Command	Description
<a href="#">show interfaces rep [detail]</a>	Displays REP configuration and status for all interfaces or the specified interface.

## reserved-only

Use the **reserved-only** DHCP pool configuration mode command to allocate only reserved addresses in the Dynamic Host Configuration Protocol (DHCP) address pool. Use the **no** form of the command to return to the default.

**reserved-only**

**no reserved-only**

**Syntax Description** This command has no arguments or keywords.

**Defaults** The default is to not restrict pool addresses

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(50)SE	This command was introduced.

**Usage Guidelines** Entering the **reserved-only** command restricts assignments from the DHCP pool to preconfigured reservations. Unreserved addresses that are part of the network or on pool ranges are not offered to the client, and other clients are not served by the pool.

By entering this command, users can configure a group of switches with DHCP pools that share a common IP subnet and that ignore requests from clients of other switches.

To access DHCP pool configuration mode, enter the **ip dhcp pool *name*** global configuration command.

**Examples** This example shows how to configure the DHCP pool to allocate only reserved addresses:

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip dhcp pool test1
Switch(dhcp-config)# reserved-only
```

You can verify your settings by entering the **show ip dhcp pool** privileged EXEC command.

Related Commands	Command	Description
	<b>show ip dhcp pool</b>	Displays the DHCP address pools.

■ reserved-only

## rmon collection stats

Use the **rmon collection stats** interface configuration command to collect Ethernet group statistics, which include usage statistics about broadcast and multicast packets, and error statistics about cyclic redundancy check (CRC) alignment errors and collisions. Use the **no** form of this command to return to the default setting.

**rmon collection stats** *index* [*owner name*]

**no rmon collection stats** *index* [*owner name*]

Syntax Description		
<i>index</i>		Remote Network Monitoring (RMON) collection control index. The range is 1 to 65535.
<i>owner name</i>		(Optional) Owner of the RMON collection.

**Defaults** The RMON statistics collection is disabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** The RMON statistics collection command is based on hardware counters. If the port is a user network interface (UNI) or enhanced network interface (ENI), you must use the **no shutdown** interface configuration command to enable it before using the **rmon collection stats** command. UNIs and ENIs are disabled by default. Network node interfaces (NNIs) are enabled by default.

**Examples** This example shows how to collect RMON statistics for the owner *root*:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# rmon collection stats 2 owner root
```

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

Related Commands	Command	Description
	<b>show rmon statistics</b>	Displays RMON statistics.

# sdm prefer

Use the **sdm prefer** global configuration command to configure the template used in Switch Database Management (SDM) resource allocation. If the switch is running the metro IP access image, you can use a template to balance resources between Layer 2 and Layer 3 functionality, or you can maximize system usage to support only Layer 2 features in hardware. You can also select the dual IPv4 and IPv6 template to support IPv6 forwarding. Use the **no** form of this command to return to the default template.

```
sdm prefer { default | dual-ipv4-and-ipv6 { default | routing | vlan } | layer-2 }
```

```
no sdm prefer
```



### Note

The **default** and **dual-ipv4-and-ipv6** keywords are visible only when the metro IP access image is installed on the switch.

### Syntax Description

<b>default</b>	Give balance to all functions.
<b>layer-2</b>	Maximizes system resources for Layer 2 functionality with no routing support.
<b>dual-ipv4-and-ipv6</b> { <b>default</b>   <b>routing</b>   <b>vlan</b> }	Select a template that supports both IPv4 and IPv6 routing. <ul style="list-style-type: none"> <li>• <b>default</b>—Provide balance to IPv4 and IPv6 Layer 2 and Layer 3 functionality.</li> <li>• <b>routing</b>—Provide maximum system usage for IPv4 and IPv6 routing, including IPv4 policy-based routing.</li> <li>• <b>vlan</b>—Provide maximum system usage for IPv4 and IPv6 VLANs.</li> </ul>

### Defaults

The default template provides a balance to all features.

On switches that are running the metro access image, only the layer-2 template is supported.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.
12.2(50)SE	The dual-ipv4-and-ipv6 templates were added.

### Usage Guidelines

You must reload the switch for the configuration to take effect. If you enter the **show sdm prefer** command before you enter the **reload** privileged EXEC command, the **show sdm prefer** command shows the template currently in use and the template that will become active after a reload.

The default templates balances the use of system resources. Do not use the default template if you do not have routing enabled on your switch. Using the balanced template prevents Layer 2 features from using the memory allocated to unicast routing in the default template.

Do not use the layer-2 template if the switch is routing packets. The layer-2 template does not support routing and forces any routing to be done through software. This overloads the CPU and severely degrades routing performance.

If you try to configure IPv6 features without first selecting a dual IPv4 and IPv6 template, a warning message appears.

The dual-stack templates provide in less allowable TCAM capacity for each resource. Do not use them if you plan to forward only IPv4 traffic.

Table 2-4 lists the approximate number of each resource supported in each of the two IPv4 templates for a switch running the metro IP access image. The values in the template are based on eight routed interfaces and approximately 1024 VLANs and represent the approximate hardware boundaries set when a template is selected. If a section of a hardware resource is full, all processing overflow is sent to the CPU, seriously impacting switch performance.

**Table 2-4** Approximate Number of Feature Resources Allowed by Each Template

Resource	Layer-2	Default
Unicast MAC addresses	8 K	5 K
IPv4 IGMP groups + multicast routes (default only)	–	1 K
IP v4 IGMP groups (layer-2 only)	1 K	–
IPv4 multicast routes (layer-2 only)	0	–
IPv4 IGMP groups and multicast routes	1 K	–
IPv4 unicast routes	0	9 K
• Directly connected IPv4 hosts	–	5 K
• Indirect IPv4 routes	–	4 K
IPv4 policy-based routing ACEs <sup>1</sup>	0	0.5 K
IPv4 or MAC QoS <sup>2</sup> ACEs	0.5 K	0.5 K
IPv4 or MAC security ACEs	1 K	1 K

1. ACEs = Access control entries.

2. QoS = Quality of service.

Table 2-5 defines the approximate feature resources allocated by each dual template. Template estimations are based on a switch with 8 routed interfaces and approximately 1000 VLANs.

**Table 2-5** Approximate Feature Resources Allowed by Dual IPv4-IPv6 Templates

Resource	IPv4-and-IPv6 Default	IPv4-and-IPv6 Routing	IPv4-and-IPv6 VLAN
Unicast MAC addresses	2 K	1.5 K	8 K
IPv4 IGMP groups and multicast routes	1 K	1 K	1 K
Total IPv4 unicast routes:	3 K	2.75 K	0
• Directly connected IPv4 hosts	2 K	1.5 K	0
• Indirect IPv4 routes	1 K	1.25 K	0
IPv6 multicast groups	1 K	1 K	1 K
Total IPv6 unicast routes:	3 K	2.75 K	0

**Table 2-5** Approximate Feature Resources Allowed by Dual IPv4-IPv6 Templates (continued)

Resource	IPv4-and-IPv6 Default	IPv4-and-IPv6 Routing	IPv4-and-IPv6 VLAN
• Directly connected IPv6 addresses	2 K	1.5 K	0
• Indirect IPv6 unicast routes	1 K	1.25 K	0
IPv4 policy-based routing ACEs	0	0.25 K	0
IPv4 or MAC QoS ACEs (total)	0.75 K	0.75 K	0.75 K
IPv4 or MAC security ACEs (total)	1 K	0.5 K	1K
IPv6 policy-based routing ACEs <sup>1</sup>	0	0.25 K	0
IPv6 QoS ACEs	0.5 K	0.5 K	0.5 K
IPv6 security ACEs	0.5 K	0.5 K	0.5 K

1. IPv6 policy-based routing is not supported.

## Examples

This example shows how to configure the layer-2 template on a switch:

```
Switch(config)# sdm prefer layer-2
Switch(config)# exit
Switch# reload
```

This is an example of an output display when you have changed the template to the layer-2 template and have not reloaded the switch:

```
Switch# show sdm prefer
The current template is "default" template.
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:          5K
number of IPv4 IGMP groups + multicast routes: 1K
number of IPv4 unicast routes:           9K
  number of directly-connected IPv4 hosts: 5K
  number of indirect IPv4 routes:         4K
number of IPv4 policy based routing aces: 0.5K
number of IPv4/MAC qos aces:              0.5K
number of IPv4/MAC security aces:         1K
On next reload, template will be "layer-2" template.
```

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

## Related Commands

Command	Description
<a href="#">show sdm prefer</a>	Displays the current SDM template in use or displays the templates that can be used, with the approximate resource allocation per feature.



## service instance

Use the **service instance** interface configuration command to configure an Ethernet service instance on the interface and to enter Ethernet service configuration mode. Use the **no** form of this command to delete the service instance.

**service instance** *id* **ethernet** [*evc-id*]

**no service instance** *id*

This command is available only if your switch is running the metro IP access or metro access image.

Syntax Description		
	<i>id</i>	Define a service instance identifier, a per-interface service identifier that does not map to a VLAN. The range is 1 to 4294967295.
	<b>ethernet</b>	Identify the service instance as an Ethernet instance.
	<i>evc-id</i>	(Optional) Attach an Ethernet virtual connection (EVC) to the service instance.

**Defaults** No Ethernet service instances are defined.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** After you enter the **service instance** *id* **ethernet** command, the switch enters Ethernet service configuration mode, and these configuration commands are available:

- **default**: sets the service instance to its default state.
- **ethernet lmi ce-vlan map**: configures Ethernet Local Management Interface (LMI) parameters. See the [ethernet lmi ce-vlan map](#) command.
- **exit**: exits EVC configuration mode and returns to global configuration mode.
- **no**: negates a command or returns a command to its default setting.

**Examples** This example shows how to define an Ethernet service instance and to enter Ethernet service configuration mode for EVC *test*:

```
Switch(config-if) # service instance 333 ethernet test
Switch(config-if-srv) #
```

■ service instance

Related Commands	Command	Description
	<a href="#">show ethernet service instance</a>	Displays information about configured Ethernet service instances.

# service password-recovery

Use the **service password-recovery** global configuration command to enable the password-recovery mechanism (the default). This mechanism allows an end user with physical access to the switch to press the break key on the console terminal to interrupt the boot process while the switch is powering up and to assign a new password.

Use the **no** form of this command to disable part of the password-recovery functionality. When the password-recovery mechanism is disabled, interrupting the boot process is allowed only if the user agrees to set the system back to the default configuration.

**service password-recovery**

**no service password-recovery**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** The password-recovery mechanism is enabled.

---

**Command Modes** Global configuration

---

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

---



---

**Usage Guidelines** As a system administrator, you can use the **no service password-recovery** command to disable some of the functionality of the password recovery feature by allowing an end user to reset a password only by agreeing to return to the default configuration. This provides configuration file security by ensuring that only authenticated and authorized users have access to the configuration file and prevents users from accessing the configuration file by using the password recovery process.

The password recovery procedure requires using a break key. After the switch performs power-on self test (POST), the switch begins the autoboot process. The boot loader prompts the user for a break key character during the boot-up sequence, as shown in this example:

```
***** The system will autoboot in 5 seconds *****
```

Send a break key to prevent autobooting.

You must enter the break key on the console terminal within 5 seconds of receiving the message that the system will autoboot. A user with physical access to the switch presses the break key on the console terminal within 5 seconds of receiving the message that flash memory is initializing. The System LED flashes green until the **break key** is accepted. After the **break key** is accepted, the System LED turns off until after the switch boots.

If the password-recovery mechanism is disabled, this message appears:

```
The password-recovery mechanism has been triggered, but
is currently disabled. Access to the boot loader prompt
through the password-recovery mechanism is disallowed at
this point. However, if you agree to let the system be
reset back to the default system configuration, access
to the boot loader prompt can still be allowed.
```

```
Would you like to reset the system back to the default configuration (y/n)?
```

If the user chooses not to reset the system to the default configuration, the normal boot process continues as if the **break key** had not been pressed. If you choose to reset the system to the default configuration, the configuration file in flash memory is deleted, and the VLAN database file, *flash:vlan.dat* (if present), is deleted.



#### Note

If you use the **no service password-recovery** command to control end user access to passwords, we recommend that you save a copy of the configuration file in a location away from the switch in case the end user uses the password recovery procedure and sets the system back to default values. Do not keep a backup copy of the configuration file on the switch.

You can enter the **show version** privileged EXEC command to determine if password recovery is enabled or disabled.

#### Examples

This example shows how to disable password recovery on a switch so that a user can only reset a password by agreeing to return to the default configuration.

```
Switch(config)# no service-password recovery
Switch(config)# exit
```

#### Related Commands

Command	Description
<a href="#">show version</a>	Displays version information for the hardware and firmware.

## service-policy (interface configuration)

Use the **service-policy** interface configuration command to apply a policy map defined by the **policy-map** command to the incoming or outgoing traffic of a physical port. 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

<b>input</b>	Apply the policy map to the input of a physical port.
<b>output</b>	Apply the policy map to the output of a physical port.
<i>policy-map-name</i>	The specified policy map to be applied.



### Note

Though visible in the command-line help strings, the **history** keyword is not supported, and you should ignore the statistics that it gathers.

### Defaults

No policy maps are attached to the port.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

Only one input policy map and one output policy map can be attached to an interface.

Beginning with Cisco IOS Release 12.2(35)SE, you can attach an output policy map to each interface on the switch. However, the switch supports a limit of three unique queue-limit configurations across all output policy maps at any time. Multiple policy maps can share the same queue-limit configuration. If you try to attach an output policy map with a fourth unique queue-limit configuration, you see this error message:

```
QoS: Configuration failed. Maximum number of allowable unique queue-limit
configurations exceeded.
```

You can attach input or output policy maps to a Fast Ethernet or Gigabit Ethernet port. You cannot attach policy maps to switch virtual interfaces (SVIs) and EtherChannel interfaces.

**Examples**

This example shows how to apply *plcmap1* as an output policy map:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output plcmap1
```

This example shows how to remove *plcmap2* from the port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no service-policy output plcmap2
```

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

**Related Commands**

Command	Description
<a href="#">policy-map</a>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
<a href="#">show policy-map</a>	Displays quality of service (QoS) policy maps.
<a href="#">show policy-map interface [interface-id]</a>	Displays policy maps configured on the specified interface or on all interfaces.
<a href="#">show running-config</a>	Displays the operating configuration.

## service-policy (policy-map class configuration)

Use the **service-policy** policy-map class configuration command to configure a quality of service (QoS) service policy for an input or output policy map or a per-port, per-VLAN policy map. Use the **no** form of this command to disable a service policy as a QoS policy within a policy map.

**service-policy** *policy-map-name*

**no service-policy** *policy-map-name*

<b>Syntax Description</b>	<i>policy-map-name</i>	Name of the service policy map (created by using the <b>policy-map</b> global configuration command) to be used in a QoS hierarchical service policy.
---------------------------	------------------------	---

<b>Defaults</b>	No service policies are defined.
-----------------	----------------------------------

<b>Command Modes</b>	Policy-map class configuration
----------------------	--------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

<b>Usage Guidelines</b>	<p>You can use the <b>service-policy input</b> command to assign a child QoS policy to a parent input policy defined with a classification based on VLAN IDs. This allows you to create a hierarchical policy for per-port, per-VLAN QoS.</p> <p>You attach a service policy created in policy-map class configuration to a parent output policy map. This creates hierarchical policy mapping. Use the <b>service-policy</b> <i>policy-map-name</i> policy-map class configuration command to enter a second-level (child) policy map.</p> <p>For an input policy map, when you configure classes with classification based on VLAN IDs by using the <b>match vlan</b> class-map configuration command, you can use <b>service-policy</b> policy-map class configuration command to associate a child QoS policy with that class. This provides the ability to apply independent QoS policies based on the VLAN IDs of the incoming traffic on the port. The per-port, per-vlan ingress QoS feature is supported only using a 2-level hierarchical input policymap, where the parent level defines the VLAN-based classification and the child level defines the QoS policy to be applied to the corresponding VLAN or VLANs. You can configure the child policy with all actions that are available for input policy maps, specifically policing and marking.</p> <p>For an output policy map, when <b>shape average</b> is also configured on the class <b>class-default</b>, you can configure hierarchical policy maps by attaching a single <b>service-policy</b> policy-map class command to the class <b>class-default</b>. This policy map specifies the service policy for the port-shaped traffic on the port and is the parent policy map. You can configure the child policy with class-based queuing actions by using the <b>queue-limit</b> policy map class command and with scheduling actions (by using the <b>bandwidth</b>, <b>shape average</b>, or <b>priority</b> command).</p> <p>To return to policy-map configuration mode, use the <b>exit</b> command. To return to privileged EXEC mode, use the <b>end</b> command.</p>
-------------------------	---

**Examples**

This example shows how to define the service policy and to attach it to a parent policy map to set the maximum bandwidth (shape) for an output queue at 90000000 bits per second:

```
Switch(config)# policy-map out-policy-parent
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 90000000
Switch(config-pmap-c)# service-policy out-policy
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

In this example, the class maps in the child-level policy map specify matching criteria for voice and video traffic, and the child policy map sets the action for input policing each type of traffic. The parent-level policy map specifies the VLANs to which the child policy maps are applied on the specified port.

```
Switch(config)# class-map match-any dscp-23 video
Switch(config-cmap)# match ip dscp 23
Switch(config-cmap)# exit
Switch(config)# class-map match-any dscp-63 voice
Switch(config-cmap)# match ip dscp-63
Switch(config-cmap)# exit
Switch(config)# class-map match-any customer-1-vlan
Switch(config-cmap)# match vlan 100
Switch(config-cmap)# match vlan 200
Switch(config-cmap)# match vlan 300
Switch(config-cmap)# exit
```

**Note**

You can also enter the match criteria as **match vlan 100 200 300** with the same result.

```
Switch(config)# policy-map child policy-1
Switch(config-pmap)# class dscp-63 voice
Switch(config-pmap-c)# police cir 10000000 bc 50000
Switch(config-pmap-c)# conform-action set-cos-transmit 5
Switch(config-pmap-c)# exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# class dscp-23 video
Switch(config-pmap-c)# set cos 4
Switch(config-pmap-c)# set ip precedence 4
Switch(config-pmap-c)# exit
```

```
Switch(config)# policy-map parent-customer-1
Switch(config-pmap)# class customer-1-vlan
Switch(config-pmap-c)# service-policy ingress-policy-1
Switch(config-pmap-c)# exit
```

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

**Related Commands**

Command	Description
<a href="#">class</a>	Defines a traffic classification match criteria for the specified class-map name.
<a href="#">policy-map</a>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
<a href="#">show policy-map</a>	Displays quality of service (QoS) policy maps.



## set cos

Use the **set cos** policy-map class configuration command to set a Layer 2 class of service (CoS) value in the packet. Use the **no** form of this command to remove traffic marking.

```
set cos {cos_value | from-field [table table-map-name]}
```

```
no set cos {cos_value | from-field [table table-map-name]}
```

Syntax Description		
<i>cos_value</i>		Enter an IEEE 802.1Q class of service/user priority value with which to classify traffic. The range is from 0 to 7.
<i>from-field</i>		Specific a packet-marking category to be used to set the CoS value of the packet. If you are using a table map for mapping and converting packet-marking values, this establishes the <i>map-from</i> packet-marking category.  These options are supported: <ul style="list-style-type: none"> <li>• <b>cos</b>—CoS value</li> <li>• <b>dscp</b>—Differentiated Services Code Point (DSCP) value.</li> <li>• <b>precedence</b>—IP-precedence value</li> </ul>
<b>table</b>		(Optional) Used in conjunction with the <i>from-field</i> keyword. Indicates that the values set in a specified table map are used to set the CoS value
<i>table-map-name</i>		(Optional) Used in conjunction with the <b>table</b> keyword. Name of the table map used to specify the CoS value. The table map name can be a maximum of 64 alphanumeric characters.

**Defaults** No traffic marking is defined.

**Command Modes** Policy-map class configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** You can configure **set cos** with all other marking actions, specifically **set dscp**, **set precedence**, and **set qos-group**, for the same class. Support was also added for the ability to configure more than one marking action with enhanced packet marking by using table maps for the same class.

Use the **set cos** command if you want to mark a packet that is being sent to a switch. Switches can leverage Layer 2 header information including a CoS value marking.

You can use the **match cos** class-map configuration command and the **set cos** policy-map class configuration command together to allow switches to interoperate and provide quality of service (QoS) based on the CoS markings. You can also configure Layer 2 to Layer 3 mapping by matching on the CoS value because switches can already match and set CoS values.

If you are using this command to perform enhanced packet marking, you can use the *from-field* packet marking option for mapping and setting the CoS value. The supported *from-field* marking categories are: CoS, DSCP, and IP precedence.

If you specify a *from-field* category, but do not specify the **table** keyword and *table-map-name*, the default action is to copy the value associated with the *from-field* category as the CoS value. For example, if you enter the **set cos precedence** command, the precedence value is copied and used as the CoS value. If you enter the **set cos dscp** command, the DSCP value is copied and used as the CoS value.

### Examples

This example shows how to set all FTP traffic to cos 3:

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set cos 3
Switch(config-pmap-c)# exit
```

This example shows how to assign a DSCP to CoS table map to a class:

```
Switch(config)# policy-map inpolicy
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set cos dscp table dscp-cos-tablemap
Switch(config-pmap)# exit
```

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

### Related Commands

Command	Description
<a href="#">class</a>	Defines a traffic classification match criteria for the specified class-map name.
<a href="#">policy-map</a>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
<a href="#">show policy-map</a>	Displays QoS policy maps.

# set dot1ad dei

Use the **set dot1ad dei** policy-map class configuration command to mark IPv4 traffic by setting a drop eligibility indicator (DEI) in the IEEE 802.1ad frame. Use the **no** form of this command to remove traffic marking.

```
set dot1ad dei dei_value
```

```
no set dot1ad dei
```

<b>Syntax Description</b>	<i>dei-value</i>	Set the DEI bit in the 802.1ad packet. The range is 0 to 1.
<b>Defaults</b>	No DEI bit value is set.	
<b>Command Modes</b>	Policy-map class configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(55)SE	This command was introduced.

**Usage Guidelines** You can use this command with per port or per-port per-VLAN policies to set the DEI bit in the 802.1ad header of the packet.

DEI marking is supported only in ingress packets.

You can set the DEI bit only on 802.1ad ports. You configure these ports by entering the **ethernet dot1ad {nni | uni {c-port | s-port | c-port isolate | s-port isolate}}** interface configuration command.

- C-UNI ports can both classify and mark on the DEI bit.
- S-UNI ports can classify and mark on the DEI bit of either the default S-tag on the port or the S-tagged packet received from the customer port.
- S-NNI ports can both classify and mark on the DEI bit.

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

**Examples** This example shows how to configure a policy map with two classes (*match\_1* and *match\_0*) that set the DEI bit:

```
Switch(config)# policy-map dei
Switch(config-pmap)# class match 1
Switch(config-pmap-c)# set set dot1ad dei1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class match 0
Switch(config-pmap-c)# set set dot1ad dei0
Switch(config-pmap-c)# exit
```

This example shows how to apply the policy map to an S-NNI port ingress:

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# ethernet dot1ad
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport
Switch(config-if)# service-policy input match-dei
```

#### Related Commands

Command	Description
<b>match dot1ad dei</b>	Defines a traffic classification match criteria to use the DEI bit.
<b>ethernet dot1ad</b>	Configures an interface as an 802.1ad C-port or S-port.
<b>show policy map</b>	Displays QoS policy maps.

# set dscp

Use the **set [ip] dscp** policy-map class configuration command to mark IPv4 traffic by setting a Differentiated Services Code Point (DSCP) value in the type of service (ToS) byte of the packet. Use the **no** form of this command to remove traffic marking.

```
set [ip] dscp {dscp_value |from-field [table table-map-name]}
```

```
no set [ip] dscp {dscp_value |from-field [table table-map-name]}
```



## Note

Entering **ip dscp** is the same as entering **dscp**.

## Syntax Description

<i>dscp-value</i>	Enter a DSCP value with which to classify traffic. The range is from 0 to 63. You also can enter a mnemonic name for a commonly used value.
<i>from-field</i>	Specific a packet-marking category to be used to set the DSCP value of the packet. If you are using a table map for mapping and converting packet-marking values, this establishes the <i>map-from</i> packet-marking category.  These options are supported: <ul style="list-style-type: none"> <li>• <b>cos</b>—class of service (CoS) value</li> <li>• <b>dscp</b>—DSCP value.</li> <li>• <b>precedence</b>—IP-precedence value</li> </ul>
<b>table</b>	(Optional) Used in conjunction with the <i>from-field</i> keyword. Indicates that the values set in a specified table map are used to set the DSCP value
<i>table-map-name</i>	(Optional) Used in conjunction with the <b>table</b> keyword. Name of the table map used to specify the DSCP value. The table map name can be a maximum of 64 alphanumeric characters.

## Defaults

No traffic marking is defined.

## Command Modes

Policy-map class configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

**Usage Guidelines**

You can configure **set dscp** with other marking actions, specifically **set cos** and **set qos-group**, for the same class. Support was also added for the ability to configure more than one marking action with enhanced packet marking by using table maps for the same class.

You cannot use the **set dscp** command with the **set precedence** command to mark the same packet. DSCP values and IP precedence values are mutually exclusive. A packet can have one value of the other, but not both.

After DSCP bits are set, other quality of service (QoS) features can then operate on the bit settings.

The network gives priority (or some type of expedited handling) to marked traffic. Typically, you set the DSCP value at the edge of the network (or administrative domain) and data is then queued according to the precedence. Class-based weighted fair queuing (CBWFQ) can speed up handling for high-precedence traffic at congestion points. Weighted Tail Drop (WTD) ensures that high-precedence traffic has lower loss rates than other traffic during times of congestion.

Instead of using numeric values, you can also specify the *dscp-value* by using the reserved keywords **EF**, **AF11**, and **AF12**.

If you are using this command to perform enhanced packet marking, you can use the *from-field* packet marking option for mapping and setting the DSCP value. The supported *from-field* marking categories are: CoS, DSCP, and IP precedence.

If you specify a *from-field* category, but do not specify the **table** keyword and *table-map-name*, the default action is to copy the value associated with the *from-field* category as the DSCP value. For example, if you enter the **set dscp cos** command, the CoS value is copied and used as the DSCP value.

**Examples**

This example shows how to set all FTP traffic to DSCP 10:

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# exit
```

This example shows how to assign a CoS to DSCP table map to a class:

```
Switch(config)# policy-map inpolicy
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set dscp cos table cos-dscp-tablemap
Switch(config-pmap)# exit
```

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

**Related Commands**

Command	Description
<b>class</b>	Defines a traffic classification match criteria for the specified class-map name.
<b>policy-map</b>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
<b>show policy-map</b>	Displays QoS policy maps.

# set precedence

Use the **set [ip] precedence** policy-map class configuration command to mark IPv4 traffic by setting an IP-precedence value in the packet. Use the **no** form of this command to remove traffic marking.

```
set [ip] precedence {precedence_value | from-field [table table-map-name]}
```

```
no set [ip] precedence {precedence_value | from-field [table table-map-name]}
```



## Note

Entering **ip precedence** is the same as entering **precedence**.

## Syntax Description

<i>precedence_value</i>	Enter an IPv4 precedence value with which to classify traffic. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.
<i>from-field</i>	Specific a packet-marking category to be used to set the precedence value of the packet. If you are using a table map for mapping and converting packet-marking values, this establishes the <i>map-from</i> packet-marking category.  These options are supported: <ul style="list-style-type: none"> <li>• <b>cos</b>—class of service (CoS) value</li> <li>• <b>dscp</b>—Differentiated Services Code Point (DSCP) value.</li> <li>• <b>precedence</b>—IP-precedence value</li> </ul>
<b>table</b>	(Optional) Used in conjunction with the <i>from-field</i> keyword. Indicates that the values set in a specified table map are used to set the precedence value
<i>table-map-name</i>	(Optional) Used in conjunction with the <b>table</b> keyword. Name of the table map used to specify the precedence value. The table map name can be a maximum of 64 alphanumeric characters.

## Defaults

No traffic marking is defined.

## Command Modes

Policy-map class configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

**Usage Guidelines**

You can configure **set precedence** with other marking actions, specifically **set cos** and **set qos-group**, for the same class. Support was also added for the ability to configure more than one marking action with enhanced packet marking by using table maps for the same class.

You cannot use the **set precedence** command with the **set dscp** command to mark the same packet. DSCP values and IP precedence values are mutually exclusive. A packet can have one value of the other, but not both.

After precedence bits are set, other quality of service (QoS) features can then operate on the bit settings.

The network gives priority (or some type of expedited handling) to marked traffic. Typically, you set the precedence value at the edge of the network (or administrative domain) and data is then queued according to the precedence. Class-based weighted fair queuing (CBWFQ) can speed up handling for high-precedence traffic at congestion points. Weighted Tail Drop (WTD) ensures that high-precedence traffic has lower loss rates than other traffic during times of congestion.

Instead of using numeric values, you can also specify the *dscp-value* by using the reserved keywords **EF**, **AF11**, and **AF12**.

If you are using this command to perform enhanced packet marking, you can use the *from-field* packet marking option for mapping and setting the precedence value. The supported *from-field* marking categories are: CoS, DSCP, and IP precedence.

If you specify a *from-field* category, but do not specify the **table** keyword and *table-map-name*, the default action is to copy the value associated with the *from-field* category as the precedence value. For example, if you enter the **set precedence cos** command, the CoS value is copied and used as the precedence value.

**Examples**

This example shows how to give all FTP traffic an IP precedence value of 5:

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set precedence 5
Switch(config-pmap-c)# exit
```

This example shows how to assign a CoS to precedence table map to a class:

```
Switch(config)# policy-map inpolicy
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set precedence cos table cos-prec-tablemap
Switch(config-pmap)# exit
```

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

**Related Commands**

Command	Description
<b>class</b>	Defines a traffic classification match criteria for the specified class-map name.
<b>policy-map</b>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
<b>show policy-map</b>	Displays QoS policy maps.



## set qos-group

Use the **set qos-group** policy-map class configuration command to set a quality of service (QoS) group identifier that can be used later to classify packets. Use the **no** form of this command to remove the group identifier.

**set qos-group** *value*

**no set qos-group** *value*

<b>Syntax Description</b>	<i>value</i>	Set the QoS group value to use to classify traffic. The range is from 0 to 99.
---------------------------	--------------	--

<b>Defaults</b>	No traffic marking is defined.
-----------------	--------------------------------

<b>Command Modes</b>	Policy-map class configuration
----------------------	--------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

**Usage Guidelines** You can configure **set qos-group** with all other marking actions, specifically **set cos**, **set dscp**, and **set precedence**, for the same class. Support was also added for the ability to configure more than one marking action with enhanced packet marking by using table maps for the same class.

Use this command to associate a QoS group value with a traffic flow as it enters the switch, which can then be used in an output policy map to identify the flow.

A maximum of 100 QoS groups (0 through 99) is supported on the switch.

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 set all FTP traffic to QoS group 5:

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set qos-group 5
Switch(config-pmap-c)# exit
```

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

■ set qos-group

Related Commands	Command	Description
	<a href="#">class</a>	Defines a traffic classification match criteria for the specified class-map name.
	<a href="#">policy-map</a>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
	<a href="#">show policy-map</a>	Displays QoS policy maps.

# setup

Use the setup privileged EXEC command to configure the switch with its initial configuration.

## setup

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** When you use the **setup** command, make sure that you have this information:

- IP address and network mask
- Password strategy for your environment

When you enter the **setup** command, an interactive dialog, called the System Configuration Dialog, appears. It guides you through the configuration process and prompts you for information. The values shown in brackets next to each prompt are the default values last set by using either the **setup** command facility or the **configure** privileged EXEC command.

Help text is provided for each prompt. To access help text, press the question mark (?) key at a prompt. To return to the privileged EXEC prompt without making changes and without running through the entire System Configuration Dialog, press **Ctrl-C**.

When you complete your changes, the setup program shows you the configuration command script that was created during the setup session. You can save the configuration in NVRAM or return to the setup program or the command-line prompt without saving it.

**Examples** This is an example of output from the **setup** command:

```
Switch# setup
--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system.

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:
```

Enter host name [Switch]:*host-name*

The enable secret is a password used to protect access to privileged EXEC and configuration modes. This password, after entered, becomes encrypted in the configuration.

Enter enable secret: *enable-secret-password*

The enable password is used when you do not specify an enable secret password, with some older software versions, and some boot images.

Enter enable password: *enable-password*

The virtual terminal password is used to protect access to the router over a network interface.

Enter virtual terminal password: *terminal-password*

Configure SNMP Network Management? [no]: **yes**

Community string [public]:

Current interface summary

Any interface listed with OK? value "NO" does not have a valid configuration

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	172.20.135.202	YES	NVRAM	up	up
GigabitEthernet0/1	unassigned	YES	unset	up	up
GigabitEthernet0/2	unassigned	YES	unset	up	down

<output truncated>

Port-channel1	unassigned	YES	unset	up	down
---------------	------------	-----	-------	----	------

Enter interface name used to connect to the management network from the above interface summary: **vlan1**

Configuring interface vlan1:

Configure IP on this interface? [yes]: **yes**

IP address for this interface: *ip\_address*

Subnet mask for this interface [255.0.0.0]: *subnet\_mask*

The following configuration command script was created:

```
hostname host-name
enable secret 5 $1$L1Bw$0Xc1wyT.PXPkuhFwqyhVi0
enable password enable-password
line vty 0 15
password terminal-password
snmp-server community public
!
no ip routing
!
interface GigabitEthernet0/1
no ip address
!
interface GigabitEthernet0/2
no ip address
!
end
```

```
Use this configuration? [yes/no]: yes
!  
[0] Go to the IOS command prompt without saving this config.  
  
[1] Return back to the setup without saving this config.  
  
[2] Save this configuration to nvram and exit.  
  
Enter your selection [2]:
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show running-config</b>	Displays the operating configuration.
<b>show version</b>	Displays version information for the hardware and firmware.

# shape average

Use the **shape average** policy-map class configuration command to configure class-based or port shaping by specifying the average traffic shaping rate. Use the command with the class **class-default** to set port shaping. Use the **no** form of this command to remove traffic shaping.

**shape average** *target bps*

**no shape average** *target bps*

<b>Syntax Description</b>	<i>target bps</i>	Target average bit rate in bits per second (bps). The range is from 64000 to 1000000000 for class-based shaping and 4000000 to 1000000000 for port shaping.
---------------------------	-------------------	---

<b>Defaults</b>	No traffic shaping is defined.
-----------------	--------------------------------

<b>Command Modes</b>	Policy-map class configuration
----------------------	--------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

**Usage Guidelines** You use the **shape average** policy-map class command to control output traffic. Shaping is not supported in input policy maps.

Traffic shaping limits the rate of transmission of data. Configuring traffic shaping for a user-defined class or **class-default** for class-based shaping sets the peak information rate (PIR) for that class. Configuring traffic shaping for the class **class-default** when it is the only class in the policy map that is attached to an interface sets the PIR for the interface (port shaping).

You cannot configure **shape average** in a class that includes priority queuing (configured with the **priority** policy-map class configuration command).

The **shape average** command uses a default queue limit for the class. You can change the queue limit by using the **queue-limit** policy-map class command, overriding the default that is set by the **shape average** command.

You cannot use the **bandwidth** policy-map class configuration command to configure class-based weighted fair queuing (CBWFQ) and the **shape average** command to configure traffic shaping for the same class.

You can configure hierarchical policy maps by attaching the **service-policy** policy-map class command to the class **class-default** only when **shape average** is also configured on the class **class-default**.

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 configure traffic shaping for outgoing traffic on a Fast Ethernet port so that *outclass1*, *outclass2*, and *outclass3* get a maximum of 50, 20, and 10 Mbps of the buffer size. The class **class-default** gets the remaining bandwidth.

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class classout1
Switch(config-pmap-c)# shape average 50000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class classout2
Switch(config-pmap-c)# shape average 20000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class classout3
Switch(config-pmap-c)# shape average 10000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if)# service-policy out-policy
```

This example shows how to configure port shaping by configuring a hierarchical policy map that shapes a port to 90 Mbps, allocated according to the *out-policy* policy map configured in the previous example.

```
Switch(config)# policy-map out-policy-parent
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 90000000
Switch(config-pmap-c)# service-policy out-policy
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

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

**Related Commands**

Command	Description
<b>class</b>	Defines a traffic classification match criteria for the specified class-map name.
<b>policy-map</b>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
<b>show policy-map</b>	Displays QoS policy maps.
<b>show policy-map interface</b> [ <i>interface-id</i> ]	Displays policy maps configured on the specified interface or on all interfaces.

# show access-lists

Use the **show access-lists** privileged EXEC command to display access control lists (ACLs) configured on the switch.

**show access-lists** [*name* | *number* | **hardware counters** | **ipc**]

Syntax Description	
<i>name</i>	(Optional) Name of the ACL.
<i>number</i>	(Optional) ACL number. The range is 1 to 2699.
<b>hardware counters</b>	(Optional) Display global hardware ACL statistics for switched and routed packets.
<b>ipc</b>	(Optional) Display Interprocess Communication (IPC) protocol access-list configuration download information.



## Note

Though visible in the command-line help strings, the **rate-limit** keywords are not supported.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The switch supports only IP standard and extended access lists. Therefore, the allowed numbers are only 1 to 199 and 1300 to 2699.



**Examples**

This is an example of output from the **show access-lists** command:

```
Switch# show access-lists
Standard IP access list 1
 10 permit 1.1.1.1
 20 permit 2.2.2.2
 30 permit any
 40 permit 0.255.255.255, wildcard bits 12.0.0.0
Standard IP access list videowizard_1-1-1-1
 10 permit 1.1.1.1
Standard IP access list videowizard_10-10-10-10
 10 permit 10.10.10.10
Extended IP access list 121
 10 permit ahp host 10.10.10.10 host 20.20.10.10 precedence routine
```

This is an example of output from the **show access-lists hardware counters** command:

```
Switch# show access-lists hardware counters
L2 ACL INPUT Statistics
  Drop:                All frame count: 855
  Drop:                All bytes count: 94143
  Drop And Log:       All frame count: 0
  Drop And Log:       All bytes count: 0
  Bridge Only:        All frame count: 0
  Bridge Only:        All bytes count: 0
  Bridge Only And Log: All frame count: 0
  Bridge Only And Log: All bytes count: 0
  Forwarding To CPU:  All frame count: 0
  Forwarding To CPU:  All bytes count: 0
  Forwarded:          All frame count: 2121
  Forwarded:          All bytes count: 180762
  Forwarded And Log:  All frame count: 0
  Forwarded And Log:  All bytes count: 0

L3 ACL INPUT Statistics
  Drop:                All frame count: 0
  Drop:                All bytes count: 0
  Drop And Log:       All frame count: 0
  Drop And Log:       All bytes count: 0
  Bridge Only:        All frame count: 0
  Bridge Only:        All bytes count: 0
  Bridge Only And Log: All frame count: 0
  Bridge Only And Log: All bytes count: 0
  Forwarding To CPU:  All frame count: 0
  Forwarding To CPU:  All bytes count: 0
  Forwarded:          All frame count: 13586
  Forwarded:          All bytes count: 1236182
  Forwarded And Log:  All frame count: 0
  Forwarded And Log:  All bytes count: 0
```

```

L2 ACL OUTPUT Statistics
  Drop:                All frame count: 0
  Drop:                All bytes count: 0
  Drop And Log:       All frame count: 0
  Drop And Log:       All bytes count: 0
  Bridge Only:        All frame count: 0
  Bridge Only:        All bytes count: 0
  Bridge Only And Log: All frame count: 0
  Bridge Only And Log: All bytes count: 0
  Forwarding To CPU:  All frame count: 0
  Forwarding To CPU:  All bytes count: 0
  Forwarded:          All frame count: 232983
  Forwarded:          All bytes count: 16825661
  Forwarded And Log:  All frame count: 0
  Forwarded And Log:  All bytes count: 0

L3 ACL OUTPUT Statistics
  Drop:                All frame count: 0
  Drop:                All bytes count: 0
  Drop And Log:       All frame count: 0
  Drop And Log:       All bytes count: 0
  Bridge Only:        All frame count: 0
  Bridge Only:        All bytes count: 0
  Bridge Only And Log: All frame count: 0
  Bridge Only And Log: All bytes count: 0
  Forwarding To CPU:  All frame count: 0
  Forwarding To CPU:  All bytes count: 0
  Forwarded:          All frame count: 514434
  Forwarded:          All bytes count: 39048748
  Forwarded And Log:  All frame count: 0
  Forwarded And Log:  All bytes count: 0

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>access-list</b>	Configures a standard or extended numbered access list on the switch.
<b>ip access list</b>	Configures a named IP access list on the switch.
<b>mac access-list extended</b>	Configures a named or numbered MAC access list on the switch.

# show archive status

Use the **show archive status** privileged EXEC command to display the status of a new image being downloaded to a switch with the HTTP or the TFTP protocol.

**show archive status**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** If you use the **archive download-sw** privileged EXEC command to download an image to a TFTP server, the output of the **show archive status** command shows the status of the download.

**Examples** These are examples of output from the **show archive status** command:

```
Switch# show archive status
IDLE: No upgrade in progress
```

```
Switch# show archive status
LOADING: Upgrade in progress
```

```
Switch# show archive status
EXTRACT: Extracting the image
```

```
Switch# show archive status
VERIFY: Verifying software
```

```
Switch# show archive status
RELOAD: Upgrade completed. Reload pending
```

Related Commands	Command	Description
	<a href="#">Command History</a>	Downloads a new image from a TFTP server to the switch.

# show arp access-list

Use the **show arp access-list** user EXEC command to display detailed information about Address Resolution Protocol (ARP) access control (lists).

**show arp access-list** [*acl-name*]

<b>Syntax Description</b>	<i>acl-name</i> (Optional) Name of the ACL.
---------------------------	---

<b>Command Modes</b>	User EXEC
----------------------	-----------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

<b>Examples</b>	This is an example of output from the <b>show arp access-list</b> command:
-----------------	--

```
Switch> show arp access-list
ARP access list rose
  permit ip 10.101.1.1 0.0.0.255 mac any
  permit ip 20.3.1.0 0.0.0.255 mac any
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
		<a href="#">arp access-list</a>
	<a href="#">deny (ARP access-list configuration)</a>	Denies an ARP packet based on matches against the Dynamic Host Configuration Protocol (DHCP) bindings.
	<a href="#">ip arp inspection filter vlan</a>	Permits ARP requests and responses from a host configured with a static IP address.
	<a href="#">permit (ARP access-list configuration)</a>	Permits an ARP packet based on matches against the DHCP bindings.

# show boot

Use the **show boot** privileged EXEC command to display the settings of the boot environment variables.

**show boot**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Examples** This is an example of output from the **show boot** command. Switch# **show boot**

```
5d05h: %SYS-5-CONFIG_I: Configured from console by console
BOOT path-list      :
Config file         : flash:/config.text
Private Config file : flash:/private-config.text
Enable Break       : no
Manual Boot        : yes
HELPER path-list   :
Auto upgrade       : yes
```

Table 2-6 describes each field in the display.

**Table 2-6** *show boot Field Descriptions*

Field	Description
BOOT path-list	Displays a semicolon separated list of executable files to try to load and execute when automatically booting.  If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory.  If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash file system.
Config file	Displays the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
Private Config file	Displays the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
Enable Break	Displays whether a break during booting is enabled or disabled. If it is set to yes, on, or 1, you can interrupt the automatic boot process by pressing the Break key on the console after the flash file system is initialized.

**Table 2-6** *show boot Field Descriptions (continued)*

Field	Description
Manual Boot	Displays whether the switch automatically or manually boots. If it is set to no or 0, the boot loader attempts to automatically boot the system. If it is set to anything else, you must manually boot the switch from the boot loader mode.
Helper path-list	Displays a semicolon separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.

Related Commands	Command	Description
	<b>boot config-file</b>	Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
	<b>boot enable-break</b>	Enables interrupting the automatic boot process.
	<b>boot manual</b>	Enables manually booting the switch during the next boot cycle.
	<b>boot private-config-file</b>	Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the private configuration.
	<b>boot system</b>	Specifies the Cisco IOS image to load during the next boot cycle.

# show cable-diagnostics tdr

Use the **show cable-diagnostics tdr** privileged EXEC command to display the Time Domain Reflector (TDR) results.

**show cable-diagnostics tdr interface** *interface-id*



## Note

TDR is supported only on the copper Ethernet 10/100 ports on the Cisco ME switch.

## Syntax Description

*interface-id* Specify the interface on which TDR was run.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

TDR is supported only on copper Ethernet 10/100 ports on the Cisco ME switch. It is not supported on small form-factor pluggable (SFP)-module ports. For more information about TDR, see the software configuration guide for this release.

## Examples

This is an example of output from the **show cable-diagnostics tdr interface** *interface-id* command on a Cisco ME switch:

```
Switch# show cable-diagnostics tdr interface fastethernet0/1
TDR test last run on: March 01 18:14:44
```

```
Interface Speed Local pair Pair length Remote pair Pair status
-----
Fa0/1     100M   Pair A    4   +/- 5 meters Pair A    Normal
          Pair B    4   +/- 5 meters Pair B    Normal
          Pair C    N/A                Pair C    N/A
          Pair D    N/A                Pair D    N/A
```

[Table 2-7](#) lists the descriptions of the fields in the **show cable-diagnostics tdr** command output.

**Table 2-7** Fields Descriptions for the show cable-diagnostics tdr Command Output

Field	Description
Interface	Interface on which TDR was run.
Speed	Speed of connection.
Local pair	Name of the pair of wires that TDR is testing on the local interface.

**Table 2-7** Fields Descriptions for the show cable-diagnostics tdr Command Output (continued)

Field	Description
Pair length	Location on the cable where the problem is, with respect to your switch. TDR can only find the location in one of these cases: <ul style="list-style-type: none"> <li>• The cable is properly connected, the link is up, and the interface speed is 100 Mbps.</li> <li>• The cable is open.</li> <li>• The cable has a short.</li> </ul>
Remote pair	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"> <li>• Normal—The pair of wires is properly connected.</li> <li>• Not completed—The test is running and is not completed.</li> <li>• Not supported—The interface does not support TDR.</li> <li>• Open—The pair of wires is open.</li> <li>• Shorted—The pair of wires is shorted.</li> <li>• ImpedanceMis—The impedance is mismatched.</li> <li>• Short/Impedance Mismatched—The impedance mismatched or the cable is short.</li> <li>• InProgress—The diagnostic test is in progress</li> </ul>

This is an example of output from the **show interface** *interface-id* command when TDR is running:

```
Switch# show interface fastethernet0/1
fastethernet0/1 is up, line protocol is up (connected: TDR in Progress)
```

This is an example of output from the **show cable-diagnostics tdr interface** *interface-id* command when TDR is not running:

```
Switch# show cable-diagnostics tdr interface fastethernet0/1
% TDR test was never issued on fa0/1
```

If an interface does not support TDR, this message appears:

```
% TDR test is not supported on switch 1
```

**Related Commands**

Command	Description
<a href="#">test cable-diagnostics tdr</a>	Enables and runs TDR on an interface.



# show class-map

Use the **show class-map** user EXEC command to display quality of service (QoS) class maps, which define the match criteria to classify traffic.

**show class-map** [*class-map-name*]

<b>Syntax Description</b>	<i>class-map-name</i> (Optional) Display the contents of the specified class map.
---------------------------	---

<b>Command Modes</b>	User EXEC
----------------------	-----------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

**Examples** This is an example of output from the **show class-map** command:

```
Switch> show class-map
Class Map match-all videowizard_10-10-10-10 (id 2)
  Match access-group name videowizard_10-10-10-10

Class Map match-any class-default (id 0)
  Match any
Class Map match-all dscp5 (id 3)
  Match ip dscp 5
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">class-map</a>	Creates a class map to be used for matching packets to the class whose name you specify.
	<a href="#">match access-group</a>	Defines the match criteria to classify traffic.

# show controllers cpu-interface

Use the **show controllers cpu-interface** privileged EXEC command to display the state of the CPU network interface ASIC and the send and receive statistics for packets reaching the CPU.

## show controllers cpu-interface

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** This display provides information that might be useful for Cisco technical support representatives troubleshooting the switch.

**Examples** This is a partial output example from the **show controllers cpu-interface** command:

```
Switch# show controllers cpu-interface
cpu-queue-frames  retrieved  dropped  invalid  hol-block
-----
rpc               4523063  0        0        0
stp               1545035  0        0        0
ipc               1903047  0        0        0
routing protocol  96145   0        0        0
L2 protocol       79596   0        0        0
remote console    0        0        0        0
sw forwarding     5756    0        0        0
host              225646  0        0        0
broadcast         46472   0        0        0
cbt-to-spt        0        0        0        0
igmp snooping     68411   0        0        0
icmp              0        0        0        0
logging           0        0        0        0
rpf-fail          0        0        0        0
queue14           0        0        0        0
cpu heartbeat     1710501  0        0        0
```

```

Supervisor ASIC receive-queue parameters
-----
queue 0 maxrecevsize 5EE pakhead 1419A20 paktail 13EAED4
queue 1 maxrecevsize 5EE pakhead 15828E0 paktail 157FBFC
queue 2 maxrecevsize 5EE pakhead 1470D40 paktail 1470FE4
queue 3 maxrecevsize 5EE pakhead 19CDDD0 paktail 19D02C8

<output truncated>

Supervisor ASIC Mic Registers
-----
MicDirectPollInfo          80000800
MicIndicationsReceived     00000000
MicInterruptsReceived      00000000
MicPcsInfo                  0001001F
MicPlbMasterConfiguration  00000000
MicRxFifosAvailable        00000000
MicRxFifosReady            0000BFFF
MicTimeOutPeriod:         FrameTOPeriod: 00000EA6 DirectTOPeriod: 00004000

<output truncated>

MicTransmitFifoInfo:
Fifo0:  StartPtrs:      038C2800      ReadPtr:      038C2C38
        WritePtrs:      038C2C38      Fifo_Flag:    8A800800
        Weights:         001E001E
Fifo1:  StartPtr:       03A9BC00      ReadPtr:      03A9BC60
        WritePtrs:       03A9BC60      Fifo_Flag:    89800400
        writeHeaderPtr:  03A9BC60
Fifo2:  StartPtr:       038C8800      ReadPtr:      038C88E0
        WritePtrs:       038C88E0      Fifo_Flag:    88800200
        writeHeaderPtr:  038C88E0
Fifo3:  StartPtr:       03C30400      ReadPtr:      03C30638
        WritePtrs:       03C30638      Fifo_Flag:    89800400
        writeHeaderPtr:  03C30638
Fifo4:  StartPtr:       03AD5000      ReadPtr:      03AD50A0
        WritePtrs:       03AD50A0      Fifo_Flag:    89800400
        writeHeaderPtr:  03AD50A0
Fifo5:  StartPtr:       03A7A600      ReadPtr:      03A7A600
        WritePtrs:       03A7A600      Fifo_Flag:    88800200
        writeHeaderPtr:  03A7A600
Fifo6:  StartPtr:       03BF8400      ReadPtr:      03BF87F0
        WritePtrs:       03BF87F0      Fifo_Flag:    89800400

<output truncated>

```

**Related Commands**

Command	Description
<a href="#">show controllers ethernet-controller</a>	Displays per-interface send and receive statistics read from the hardware or the interface internal registers.
<a href="#">show interfaces</a>	Displays the administrative and operational status of all interfaces or a specified interface.

# show controllers ethernet-controller

Use the **show controllers ethernet-controller** privileged EXEC command without keywords to display per-interface send and receive statistics read from the hardware. Use with the **phy** keyword to display the interface internal registers or the **port-asic** keyword to display information about the port ASIC.

```
show controllers ethernet-controller [interface-id] [phy [detail]] [port-asic { configuration | statistics}]
```

## Syntax Description

<i>interface-id</i>	The physical interface (including type, module, and port number).
<b>phy</b>	(Optional) Display the status of the internal registers on the switch physical layer device (PHY) for the device or the interface. This display includes the operational state of the automatic medium-dependent interface crossover (Auto-MDIX) feature on an interface.
<b>detail</b>	(Optional) Display details about the PHY internal registers.
<b>port-asic</b>	(Optional) Display information about the port ASIC internal registers.
<b>configuration</b>	Display port ASIC internal register configuration.
<b>statistics</b>	Display port ASIC statistics, including the Rx/Sup Queue and miscellaneous statistics.

## Command Modes

Privileged EXEC (only supported with the *interface-id* keywords in user EXEC mode)

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

This display without keywords provides traffic statistics, basically the RMON statistics for all interfaces or for the specified interface.

When you enter the **phy** or **port-asic** keywords, the displayed information is useful primarily for Cisco technical support representatives troubleshooting the switch.

**Examples**

This is an example of output from the **show controllers ethernet-controller** command for an interface. [Table 2-8](#) describes the *Transmit* fields, and [Table 2-9](#) describes the *Receive* fields.

```
Switch# show controllers ethernet-controller gigabitEthernet0/1
Transmit GigabitEthernet0/1          Receive
0 Bytes                               0 Bytes
0 Unicast frames                      0 Unicast frames
0 Multicast frames                    0 Multicast frames
0 Broadcast frames                    0 Broadcast frames
0 Too old frames                      0 Unicast bytes
0 Deferred frames                     0 Multicast bytes
0 MTU exceeded frames                 0 Broadcast bytes
0 1 collision frames                  0 Alignment errors
0 2 collision frames                  0 FCS errors
0 3 collision frames                  0 Oversize frames
0 4 collision frames                  0 Undersize frames
0 5 collision frames                  0 Collision fragments
0 6 collision frames
0 7 collision frames                  0 Minimum size frames
0 8 collision frames                  0 65 to 127 byte frames
0 9 collision frames                  0 128 to 255 byte frames
0 10 collision frames                 0 256 to 511 byte frames
0 11 collision frames                 0 512 to 1023 byte frames
0 12 collision frames                 0 1024 to 1518 byte frames
0 13 collision frames                 0 Overrun frames
0 14 collision frames                 0 Pause frames
0 15 collision frames                 0 Symbol error frames
0 Excessive collisions
0 Late collisions                     0 Invalid frames, too large
0 VLAN discard frames                 0 Valid frames, too large
0 Excess defer frames                 0 Invalid frames, too small
0 64 byte frames                      0 Valid frames, too small
0 127 byte frames
0 255 byte frames                     0 Too old frames
0 511 byte frames                     0 Valid oversize frames
0 1023 byte frames                    0 System FCS error frames
0 1518 byte frames                    0 RxPortFifoFull drop frame
0 Too large frames
0 Good (1 coll) frames
```

**Table 2-8** *Transmit Field Descriptions*

Field	Description
Bytes	The total number of bytes sent on an interface.
Unicast Frames	The total number of frames sent to unicast addresses.
Multicast frames	The total number of frames sent to multicast addresses.
Broadcast frames	The total number of frames sent to broadcast addresses.
Too old frames	The number of frames dropped on the egress port because the packet aged out.
Deferred frames	The number of frames that are not sent after the time exceeds 2*maximum-packet time.
MTU exceeded frames	The number of frames that are larger than the maximum allowed frame size.
1 collision frames	The number of frames that are successfully sent on an interface after one collision occurs.
2 collision frames	The number of frames that are successfully sent on an interface after two collisions occur.
3 collision frames	The number of frames that are successfully sent on an interface after three collisions occur.
4 collision frames	The number of frames that are successfully sent on an interface after four collisions occur.

**Table 2-8** Transmit Field Descriptions (continued)

Field	Description
5 collision frames	The number of frames that are successfully sent on an interface after five collisions occur.
6 collision frames	The number of frames that are successfully sent on an interface after six collisions occur.
7 collision frames	The number of frames that are successfully sent on an interface after seven collisions occur.
8 collision frames	The number of frames that are successfully sent on an interface after eight collisions occur.
9 collision frames	The number of frames that are successfully sent on an interface after nine collisions occur.
10 collision frames	The number of frames that are successfully sent on an interface after ten collisions occur.
11 collision frames	The number of frames that are successfully sent on an interface after 11 collisions occur.
12 collision frames	The number of frames that are successfully sent on an interface after 12 collisions occur.
13 collision frames	The number of frames that are successfully sent on an interface after 13 collisions occur.
14 collision frames	The number of frames that are successfully sent on an interface after 14 collisions occur.
15 collision frames	The number of frames that are successfully sent on an interface after 15 collisions occur.
Excessive collisions	The number of frames that could not be sent on an interface after 16 collisions occur.
Late collisions	After a frame is sent, the number of frames dropped because late collisions were detected while the frame was sent.
VLAN discard frames	The number of frames dropped on an interface because the CFI <sup>1</sup> bit is set.
Excess defer frames	The number of frames that are not sent after the time exceeds the maximum-packet time.
64 byte frames	The total number of frames sent on an interface that are 64 bytes.
127 byte frames	The total number of frames sent on an interface that are from 65 to 127 bytes.
255 byte frames	The total number of frames sent on an interface that are from 128 to 255 bytes.
511 byte frames	The total number of frames sent on an interface that are from 256 to 511 bytes.
1023 byte frames	The total number of frames sent on an interface that are from 512 to 1023 bytes.
1518 byte frames	The total number of frames sent on an interface that are from 1024 to 1518 bytes.
Too large frames	The number of frames sent on an interface that are larger than the maximum allowed frame size.
Good (1 coll) frames	The number of frames that are successfully sent on an interface after one collision occurs. This value does not include the number of frames that are not successfully sent after one collision occurs.

1. CFI = Canonical Format Indicator

**Table 2-9** Receive Field Descriptions

Field	Description
Bytes	The total amount of memory (in bytes) used by frames received on an interface, including the FCS <sup>1</sup> value and the incorrectly formed frames. This value excludes the frame header bits.
Unicast frames	The total number of frames successfully received on the interface that are directed to unicast addresses.
Multicast frames	The total number of frames successfully received on the interface that are directed to multicast addresses.
Broadcast frames	The total number of frames successfully received on an interface that are directed to broadcast addresses.

**Table 2-9** Receive Field Descriptions (continued)

Field	Description
Unicast bytes	The total amount of memory (in bytes) used by unicast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
Multicast bytes	The total amount of memory (in bytes) used by multicast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
Broadcast bytes	The total amount of memory (in bytes) used by broadcast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
Alignment errors	The total number of frames received on an interface that have alignment errors.
FCS errors	The total number of frames received on an interface that have a valid length (in bytes) but do not have the correct FCS values.
Oversize frames	The number of frames received on an interface that are larger than the maximum allowed frame size.
Undersize frames	The number of frames received on an interface that are smaller than 64 bytes.
Collision fragments	The number of collision fragments received on an interface.
Minimum size frames	The total number of frames that are the minimum frame size.
65 to 127 byte frames	The total number of frames that are from 65 to 127 bytes.
128 to 255 byte frames	The total number of frames that are from 128 to 255 bytes.
256 to 511 byte frames	The total number of frames that are from 256 to 511 bytes.
512 to 1023 byte frames	The total number of frames that are from 512 to 1023 bytes.
1024 to 1518 byte frames	The total number of frames that are from 1024 to 1518 bytes.
Overrun frames	The total number of overrun frames received on an interface.
Pause frames	The number of pause frames received on an interface.
Symbol error frames	The number of frames received on an interface that have symbol errors.
Invalid frames, too large	The number of frames received that were larger than maximum allowed MTU <sup>2</sup> size (including the FCS bits and excluding the frame header) and that have either an FCS error or an alignment error.
Valid frames, too large	The number of frames received on an interface that are larger than the maximum allowed frame size.
Invalid frames, too small	The number of frames received that are smaller than 64 bytes (including the FCS bits and excluding the frame header) and that have either an FCS error or an alignment error.
Valid frames, too small	The number of frames received on an interface that are smaller than 64 bytes (or 68 bytes for VLAN-tagged frames) and that have valid FCS values. The frame size includes the FCS bits but excludes the frame header bits.
Too old frames	The number of frames dropped on the ingress port because the packet aged out.
Valid oversize frames	The number of frames received on an interface that are larger than the maximum allowed frame size and have valid FCS values. The frame size includes the FCS value but does not include the VLAN tag.

Table 2-9 Receive Field Descriptions (continued)

Field	Description
System FCS error frames	The total number of frames received on an interface that have a valid length (in bytes) but that do not have the correct FCS values.
RxPortFifoFull drop frames	The total number of frames received on an interface that are dropped because the ingress queue is full.

1. FCS = frame check sequence
2. MTU = maximum transmission unit

This is an example of output from the **show controllers ethernet-controller phy** command for a specific interface. Note that the last line of the display is the setting for Auto-MDIX for the interface.

```
Switch# show controllers ethernet-controller gigabitEthernet0/2 phy
Control Register          : 0001 0001 0100 0000
Control STATUS           : 0111 1001 0100 1001
Phy ID 1                  : 0000 0001 0100 0001
Phy ID 2                  : 0000 1100 0010 0100
Auto-Negotiation Advertisement : 0000 0011 1110 0001
Auto-Negotiation Link Partner : 0000 0000 0000 0000
Auto-Negotiation Expansion Reg : 0000 0000 0000 0100
Next Page Transmit Register : 0010 0000 0000 0001
Link Partner Next page Register : 0000 0000 0000 0000
1000BASE-T Control Register : 0000 1111 0000 0000
1000BASE-T Status Register  : 0100 0000 0000 0000
Extended Status Register   : 0011 0000 0000 0000
PHY Specific Control Register : 0000 0000 0111 1000
PHY Specific Status Register : 1000 0001 0100 0000
Interrupt Enable           : 0000 0000 0000 0000
Interrupt Status           : 0000 0000 0100 0000
Extended PHY Specific Control : 0000 1100 0110 1000
Receive Error Counter      : 0000 0000 0000 0000
Reserved Register 1        : 0000 0000 0000 0000
Global Status              : 0000 0000 0000 0000
LED Control                : 0100 0001 0000 0000
Manual LED Override        : 0000 1000 0010 1010
Extended PHY Specific Control : 0000 0000 0001 1010
Disable Receiver 1         : 0000 0000 0000 1011
Disable Receiver 2         : 1000 0000 0000 0100
Extended PHY Specific Status : 1000 0100 1000 0000
Auto-MDIX                  : On [AdminState=1 Flags=0x00052248]
```

This is an example of output from the **show controllers ethernet-controller port-asic configuration** command:

```
Switch# show controllers ethernet-controller port-asic configuration
=====
PortASIC 0 Registers
-----
DeviceType                : 000101BC
Reset                     : 00000000
PmadMicConfig             : 00000001
PmadMicDiag               : 00000003
SupervisorReceiveFifoSramInfo : 000007D0 000007D0 40000000
SupervisorTransmitFifoSramInfo : 000001D0 000001D0 40000000
GlobalStatus              : 00000800
IndicationStatus          : 00000000
IndicationStatusMask      : FFFFFFFF
InterruptStatus           : 00000000
InterruptStatusMask       : 01FFE800
```



```

SupervisorDiag                : 00000000
SupervisorFrameSizeLimit     : 000007C8
SupervisorBroadcast          : 000A0F01
GeneralIO                     : 000003F9 00000000 00000004
StackPcsInfo                  : FFFF1000 860329BD 5555FFFF FFFFFFFF
                              FF0FFF00 86020000 5555FFFF 00000000
StackRacInfo                   : 73001630 00000003 7F001644 00000003
                              24140003 FD632B00 18E418E0 FFFFFFFF

StackControlStatus            : 18E418E0
stackControlStatusMask        : FFFFFFFF
TransmitBufferFreeListInfo     : 00000854 00000800 00000FF8 00000000
                              0000088A 0000085D 00000FF8 00000000
TransmitRingFifoInfo           : 00000016 00000016 40000000 00000000
                              0000000C 0000000C 40000000 00000000
TransmitBufferInfo             : 00012000 00000FFF 00000000 00000030
TransmitBufferCommonCount      : 00000F7A
TransmitBufferCommonCountPeak : 0000001E
TransmitBufferCommonCommonEmpty : 000000FF
NetworkActivity                : 00000000 00000000 00000000 02400000
DroppedStatistics              : 00000000
FrameLengthDeltaSelect         : 00000001
SneakPortFifoInfo              : 00000000
MacInfo                        : 0EC0801C 00000001 0EC0801B 00000001
                              00C0001D 00000001 00C0001E 00000001

```

<output truncated>

This is an example of output from the **show controllers ethernet-controller port-asic statistics** command:

```

Switch# show controllers ethernet-controller port-asic statistics
=====
PortASIC 0 Statistics
-----
      0 RxQ-0, wt-0 enqueue frames          0 RxQ-0, wt-0 drop frames
4118966 RxQ-0, wt-1 enqueue frames          0 RxQ-0, wt-1 drop frames
      0 RxQ-0, wt-2 enqueue frames          0 RxQ-0, wt-2 drop frames

      0 RxQ-1, wt-0 enqueue frames          0 RxQ-1, wt-0 drop frames
    296 RxQ-1, wt-1 enqueue frames          0 RxQ-1, wt-1 drop frames
2836036 RxQ-1, wt-2 enqueue frames          0 RxQ-1, wt-2 drop frames

      0 RxQ-2, wt-0 enqueue frames          0 RxQ-2, wt-0 drop frames
      0 RxQ-2, wt-1 enqueue frames          0 RxQ-2, wt-1 drop frames
158377 RxQ-2, wt-2 enqueue frames          0 RxQ-2, wt-2 drop frames

      0 RxQ-3, wt-0 enqueue frames          0 RxQ-3, wt-0 drop frames
      0 RxQ-3, wt-1 enqueue frames          0 RxQ-3, wt-1 drop frames
      0 RxQ-3, wt-2 enqueue frames          0 RxQ-3, wt-2 drop frames

15 TxBufferFull Drop Count                0 Rx Fcs Error Frames
  0 TxBufferFrameDesc BadCrc16            0 Rx Invalid Oversize Frames
  0 TxBuffer Bandwidth Drop Cou           0 Rx Invalid Too Large Frames
  0 TxQueue Bandwidth Drop Coun           0 Rx Invalid Too Large Frames
  0 TxQueue Missed Drop Statist           0 Rx Invalid Too Small Frames
74 RxBuffer Drop DestIndex Cou            0 Rx Too Old Frames
  0 SneakQueue Drop Count                  0 Tx Too Old Frames
  0 Learning Queue Overflow Fra            0 System Fcs Error Frames
  0 Learning Cam Skip Count

15 Sup Queue 0 Drop Frames                 0 Sup Queue 8 Drop Frames
  0 Sup Queue 1 Drop Frames                 0 Sup Queue 9 Drop Frames
  0 Sup Queue 2 Drop Frames                 0 Sup Queue 10 Drop Frames

```

■ **show controllers ethernet-controller**

```

0 Sup Queue 3 Drop Frames          0 Sup Queue 11 Drop Frames
0 Sup Queue 4 Drop Frames          0 Sup Queue 12 Drop Frames
0 Sup Queue 5 Drop Frames          0 Sup Queue 13 Drop Frames
0 Sup Queue 6 Drop Frames          0 Sup Queue 14 Drop Frames
0 Sup Queue 7 Drop Frames          0 Sup Queue 15 Drop Frames
=====
PortASIC 1 Statistics
-----
0 RxQ-0, wt-0 enqueue frames      0 RxQ-0, wt-0 drop frames
52 RxQ-0, wt-1 enqueue frames     0 RxQ-0, wt-1 drop frames
0 RxQ-0, wt-2 enqueue frames      0 RxQ-0, wt-2 drop frames

<output truncated>

```

**Related Commands**

Command	Description
<a href="#">show controllers cpu-interface</a>	Displays the state of the CPU network ASIC and send and receive statistics for packets reaching the CPU.
<a href="#">show controllers tcam</a>	Displays the state of registers for all ternary content addressable memory (TCAM) in the system and for TCAM interface ASICs that are CAM controllers.

# show controllers tcam

Use the **show controllers tcam** privileged EXEC command to display the state of the registers for all ternary content addressable memory (TCAM) in the system and for all TCAM interface ASICs that are CAM controllers.

**show controllers tcam [asic [number]] [detail]**

Syntax Description	asic	(Optional) Display port ASIC TCAM information.
	<b>number</b>	(Optional) Display information for the specified port ASIC number. The range is from 0 to 15.
	<b>detail</b>	(Optional) Display detailed TCAM register information.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** This display provides information that might be useful for Cisco technical support representatives troubleshooting the switch.

**Examples** This is an example of output from the **show controllers tcam** command:

```
Switch# show controllers tcam
```

```
-----
TCAM-0 Registers
-----
```

```
REV:      00B30103
SIZE:     00080040
ID:       00000000
CCR:      00000000_F0000020

RPID0:    00000000_00000000
RPID1:    00000000_00000000
RPID2:    00000000_00000000
RPID3:    00000000_00000000
```

■ **show controllers tcam**

```
HRR0: 00000000_E000CAFC
HRR1: 00000000_00000000
HRR2: 00000000_00000000
HRR3: 00000000_00000000
HRR4: 00000000_00000000
HRR5: 00000000_00000000
HRR6: 00000000_00000000
HRR7: 00000000_00000000
<output truncated>
```

```
GMR31: FF_FFFFFFFF_FFFFFFFF
GMR32: FF_FFFFFFFF_FFFFFFFF
GMR33: FF_FFFFFFFF_FFFFFFFF
```

```
=====
TCAM related PortASIC 1 registers
=====
```

```
LookupType: 89A1C67D_24E35F00
LastCamIndex: 0000FFE0
LocalNoMatch: 000069E0
ForwardingRamBaseAddress:
                                00022A00 0002FE00 00040600 0002FE00 0000D400
                                00000000 003FBA00 00009000 00009000 00040600
                                00000000 00012800 00012900
```

**Related Commands**

Command	Description
<a href="#">show controllers cpu-interface</a>	Displays the state of the CPU network ASIC and send and receive statistics for packets reaching the CPU.
<a href="#">show controllers ethernet-controller</a>	Displays per-interface send and receive statistics read from the hardware or the interface internal registers.

# show controllers utilization

Use the **show controllers utilization** user EXEC command to display bandwidth utilization on the switch or specific ports.

**show controllers** [*interface-id*] **utilization**

<b>Syntax Description</b>	<i>interface-id</i> (Optional) ID of the switch interface.
---------------------------	--

<b>Command Modes</b>	User EXEC
----------------------	-----------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

## Examples

This is an example of output from the **show controllers utilization** command.

```
Switch> show controllers utilization
Port          Receive Utilization  Transmit Utilization
Fa0/1         0                    0
Fa0/2         0                    0
Fa0/3         0                    0
Fa0/4         0                    0
Fa0/5         0                    0
Fa0/6         0                    0
Fa0/7         0                    0
```

<output truncated>

```
Switch Receive Bandwidth Percentage Utilization : 0
Switch Transmit Bandwidth Percentage Utilization : 0
```

```
Switch Fabric Percentage Utilization : 0
```

This is an example of output from the **show controllers utilization** command on a specific port:

```
Switch> show controllers gigabitethernet0/1 utilization
Receive Bandwidth Percentage Utilization : 0
Transmit Bandwidth Percentage Utilization : 0
```

**Table 2-10** *show controllers utilization* Field Descriptions

Field	Description
Receive Bandwidth Percentage Utilization	Displays the received bandwidth usage of the switch, which is the sum of the received traffic on all the ports divided by the switch receive capacity.

**Table 2-10** *show controllers utilization Field Descriptions*

Field	Description
Transmit Bandwidth Percentage Utilization	Displays the transmitted bandwidth usage of the switch, which is the sum of the transmitted traffic on all the ports divided it by the switch transmit capacity.
Fabric Percentage Utilization	Displays the average of the transmitted and received bandwidth usage of the switch.

**Related Commands**

Command	Description
<a href="#">show controllers ethernet-controller</a>	Displays the interface internal registers.

# show cpu traffic qos

Use the **show cpu traffic qos** command in user EXEC mode to display the QoS marking values for CPU-generated traffic.

**show cpu traffic qos**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Displays output the QoS marking values for all CPU-generated traffic.

## Command Modes

User EXEC

## Command History

Release	Modification
12.2(52)SE	This command was introduced.

## Examples

The following is sample output from the **show cpu traffic qos** command:

```
Switch> show cpu traffic qos
QOS - CPU Generated Traffic
-----
Set parameter-type      To parameter-value/From
      parameter-type based on table-map
-----
Cos                      cos
      precedence table-map map1
DSCP                     Default
Precedence              dscp
Qos Group                5
```

## Related Commands

Command	Description
<a href="#">class-map</a>	Configures a class map to be used for matching packets to a specified criteria and enters class-map configuration mode.
<a href="#">cpu traffic qos cos</a>	Configures class of service (CoS) marking for control plane traffic.
<a href="#">cpu traffic qos dscp</a>	Configures quality of service (QoS) marking based on DSCP for control plane traffic.
<a href="#">cpu traffic qos precedence</a>	Configure quality of service (QoS) marking based on precedence for control plane traffic.
<a href="#">cpu traffic qos qos-group</a>	Maps <i>all</i> CPU-generated traffic to a single class in the output policy-maps without changing the class of service (CoS), IP differentiated services code point (DSCP), or IP-precedence packet markings.
<a href="#">policy-map</a>	Configures a policy map that can be attached to multiple physical ports and enters policy-map configuration mode.

Command	Description
<a href="#">show policy-map</a>	Displays QoS policy map information for the specified policy map name, interface, input or output policy maps, or policy-map class.
<a href="#">show running-config</a>	Displays the configured class maps, policy maps, table maps, and aggregate policers.
<a href="#">Related Commands</a>	Displays information for all configured table maps or the specified table map.
<a href="#">table-map</a>	Configures quality of service (QoS) mapping and enters table-map configuration mode.



# show diagnostic

Use the **show diagnostic** user EXEC command to display the online diagnostic test results and the supported test suites.

**show diagnostic content**

**show diagnostic post**

**show diagnostic result** [test {*name* | *test-id* | *test-id-range* | **all**}] [**detail**]

**show diagnostic schedule**

**show diagnostic status**

**show diagnostic switch** [**detail**]

Syntax Description	
<b>content</b>	Display test information including the test ID, the test attributes, and the supported coverage test levels for specific tests and for switches.
<b>post</b>	Display the power-on self-test (POST) results.
<b>result</b>	Display the diagnostic test results.
<b>test</b>	(Optional) Specify the test results to display: <ul style="list-style-type: none"> <li>• <i>name</i>—Enter the name of the diagnostic test to display results only for this test.</li> <li>• <i>test-id</i>—Enter the test ID number to display results only for this test. The test ID can be from 1 to 6.</li> <li>• <i>test-id-range</i>—Enter the range of test ID numbers to display results only for these tests.</li> <li>• <b>all</b>—Enter this keyword to display results for all the tests.</li> </ul>
<b>detail</b>	(Optional) Display the detailed test results.
<b>schedule</b>	Display the scheduled diagnostic tests.
<b>status</b>	Display the running diagnostic tests.
<b>switch</b>	Display diagnostic results for the switch.

**Defaults** This command has no default setting.

**Command Modes** User EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines**

The **show diagnostic post** command output is the same as the **show post** command output.

The **show diagnostic result [detail]** command output is the same as the **show diagnostic switch [detail]** command output.

**Examples**

This example shows how to display the diagnostic test IDs and attributes.

```
Switch> show diagnostic content
:
Diagnostics test suite attributes:
  B/* - Basic ondemand test / NA
  P/V/* - Per port test / Per device test / NA
  D/N/* - Disruptive test / Non-disruptive test / NA
  S/* - Only applicable to standby unit / NA
  X/* - Not a health monitoring test / NA
  F/* - Fixed monitoring interval test / NA
  E/* - Always enabled monitoring test / NA
  A/I - Monitoring is active / Monitoring is inactive
  R/* - Switch will reload after test list completion / NA
  P/* - will partition stack / NA
```

ID	Test Name	Attributes	Test Interval day hh:mm:ss.ms	Thre- shold
1)	TestPortAsicStackPortLoopback	----> B*N****I**	not configured	n/a
2)	TestPortAsicLoopback	-----> B*D*X**IR*	not configured	n/a
3)	TestPortAsicCam	-----> B*D*X**IR*	not configured	n/a
4)	TestPortAsicRingLoopback	-----> B*D*X**IR*	not configured	n/a
5)	TestMicRingLoopback	-----> B*D*X**IR*	not configured	n/a
6)	TestPortAsicMem	-----> B*D*X**IR*	not configured	n/a

This example shows how to display the diagnostic test results for a switch. You can also use the **show diagnostic switch** command to display these results.

```
Switch> show diagnostic result
SerialNo : ME3400E44

Overall diagnostic result: PASS

Test results: (. = Pass, F = Fail, U = Untested)

1) TestPortAsicStackPortLoopback ---> .
2) TestPortAsicLoopback -----> U
3) TestPortAsicCam -----> U
4) TestPortAsicRingLoopback -----> U
5) TestMicRingLoopback -----> U
6) TestPortAsicMem -----> U
```

This example shows how to display the running tests in a switch:

```
Switch> show diagnostic status
<BU> - Bootup Diagnostics, <HM> - Health Monitoring Diagnostics,
<OD> - OnDemand Diagnostics, <SCH> - Scheduled Diagnostics
=====
Card   Description                               Current Running Test           Run by
-----
1      N/A                                         N/A                             N/A
2      TestPortAsicStackPortLoopback             TestPortAsicStackPortLoopback  <OD>
      TestPortAsicLoopback                     TestPortAsicLoopback           <OD>
      TestPortAsicCam                           TestPortAsicCam                 <OD>
      TestPortAsicRingLoopback                 TestPortAsicRingLoopback       <OD>
      TestMicRingLoopback                      TestMicRingLoopback            <OD>
      TestPortAsicMem                           TestPortAsicMem                 <OD>
3      N/A                                         N/A                             N/A
4      N/A                                         N/A                             N/A
=====
<output truncated>
```

This example shows how to display the online diagnostic test schedule for a switch:

```
Switch> show diagnostic schedule
Current Time = 14:39:49 PST Tue Jul 5 2005
Diagnostic for Switch 1:
Schedule #1:
To be run daily 12:00
Test ID(s) to be executed: 1.
```

This example shows how to display the detailed results for a switch. You can also use the **show diagnostic result all detail** command to display these results.

```
Switch> show diagnostic switch detail
Switch:   SerialNo : ME3400E44

Overall diagnostic result: PASS

Test results: (. = Pass, F = Fail, U = Untested)

-----

1) TestPortAsicStackPortLoopback ---> .

Error code -----> 0 (DIAG_SUCCESS)
Total run count -----> 19
Last test execution time ----> Mar 01 1993 00:21:46
First test failure time ----> n/a
Last test failure time ----> n/a
Last test pass time -----> Mar 01 1993 00:21:46
Total failure count -----> 0
Consecutive failure count ---> 0

-----

2) TestPortAsicLoopback -----> U

Error code -----> 0 (DIAG_SUCCESS)
Total run count -----> 0
Last test execution time ----> n/a
First test failure time ----> n/a
Last test failure time ----> n/a
Last test pass time -----> n/a
Total failure count -----> 0
Consecutive failure count ---> 0
```

---

```

3) TestPortAsicCam -----> U

   Error code -----> 0 (DIAG_SUCCESS)
   Total run count -----> 0
   Last test execution time ----> n/a
   First test failure time -----> n/a
   Last test failure time -----> n/a
   Last test pass time -----> n/a
   Total failure count -----> 0
   Consecutive failure count ---> 0

```

---

```

4) TestPortAsicRingLoopback -----> U

   Error code -----> 0 (DIAG_SUCCESS)
   Total run count -----> 0
   Last test execution time ----> n/a
   First test failure time -----> n/a
   Last test failure time -----> n/a
   Last test pass time -----> n/a
   Total failure count -----> 0
   Consecutive failure count ---> 0

```

---

```

5) TestMicRingLoopback -----> U

   Error code -----> 0 (DIAG_SUCCESS)
   Total run count -----> 0
   Last test execution time ----> n/a
   First test failure time -----> n/a
   Last test failure time -----> n/a
   Last test pass time -----> n/a
   Total failure count -----> 0
   Consecutive failure count ---> 0

```

---

```

6) TestPortAsicMem -----> U

   Error code -----> 0 (DIAG_SUCCESS)
   Total run count -----> 0
   Last test execution time ----> n/a
   First test failure time -----> n/a
   Last test failure time -----> n/a
   Last test pass time -----> n/a
   Total failure count -----> 0
   Consecutive failure count ---> 0

```

---

**Related Commands**

Command	Description
<a href="#">diagnostic monitor</a>	Configures the health-monitoring diagnostic test.
<a href="#">diagnostic schedule test</a>	Sets the scheduling of test-based online diagnostic testing.
<a href="#">diagnostic start test</a>	Starts the online diagnostic test.

# show dot1q-tunnel

Use the **show dot1q-tunnel** user EXEC command to display information about IEEE 802.1Q tunnel ports.

**show dot1q-tunnel** [**interface** *interface-id*]

This command is visible only when the switch is running the metro IP access or metro access image.

<b>Syntax Description</b>	<b>interface</b> <i>interface-id</i> (Optional) Specify the interface for which to display IEEE 802.1Q tunneling information. Valid interfaces include physical ports and port channels.						
<b>Command Modes</b>	User EXEC						
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(44)EY</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(44)EY	This command was introduced.		
Release	Modification						
12.2(44)EY	This command was introduced.						
<b>Examples</b>	<p>These are examples of output from the <b>show dot1q-tunnel</b> commands:</p> <pre>Switch&gt; show dot1q-tunnel dot1q-tunnel mode LAN Port(s) ----- Gi0/1 Gi0/2 Gi0/3 Gi0/6 Po2  Switch&gt; show dot1q-tunnel interface gigabitethernet0/1 dot1q-tunnel mode LAN Port(s) ----- Gi0/1</pre>						
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><a href="#">show vlan dot1q tag native</a></td> <td>Displays 802.1Q native VLAN tagging status.</td> </tr> <tr> <td><a href="#">switchport mode dot1q-tunnel</a></td> <td>Configures an interface as an IEEE 802.1Q tunnel port.</td> </tr> </tbody> </table>	Command	Description	<a href="#">show vlan dot1q tag native</a>	Displays 802.1Q native VLAN tagging status.	<a href="#">switchport mode dot1q-tunnel</a>	Configures an interface as an IEEE 802.1Q tunnel port.
Command	Description						
<a href="#">show vlan dot1q tag native</a>	Displays 802.1Q native VLAN tagging status.						
<a href="#">switchport mode dot1q-tunnel</a>	Configures an interface as an IEEE 802.1Q tunnel port.						

# show dot1x

Use the **show dot1x** privileged EXEC command to display IEEE 802.1x statistics, administrative status, and operational status for the switch or for the specified port.

**show dot1x** [**all** | **interface** *interface-id* | **statistics interface** *interface-id*]

Syntax Description	
<b>all</b>	(Optional) Display the IEEE 802.1x status for all ports.
<b>interface</b> <i>interface-id</i>	(Optional) Display the IEEE 802.1x status for the specified port (including type, module, and port number).
<b>statistics interface</b> <i>interface-id</i>	(Optional) Display IEEE 802.1x statistics for the specified port (including type, module, and port number).

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** If you do not specify a port, global parameters and a summary appear. If you specify a port, details for that port appear.

**Examples** This is an example of output from the **show dot1x** and the **show dot1x all** privileged EXEC commands:

```
Switch# show dot1x
Sysauthcontrol                = Enabled
Dot1x Protocol Version        = 1
Dot1x Oper Controlled Directions = Both
Dot1x Admin Controlled Directions = Both
```

```
Switch# show dot1x all
Dot1x Info for interface GigabitEthernet0/1
-----
```

```
Supplicant MAC 00d0.b71b.35de
  AuthSM State      = CONNECTING
  BendSM State      = IDLE
PortStatus          = UNAUTHORIZED
MaxReq              = 2
HostMode            = Single
Port Control        = Auto
QuietPeriod         = 60 Seconds
Re-authentication   = Disabled
ReAuthPeriod        = 3600 Seconds
ServerTimeout       = 30 Seconds
SuppTimeout         = 30 Seconds
TxPeriod            = 30 Seconds
Guest-Vlan          = 0
```

```
Dot1x Info for interface GigabitEthernet0/2
-----
```

```

PortStatus      = UNAUTHORIZED
MaxReq          = 2
HostMode        = Multi
Port Control    = Auto
QuietPeriod     = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod    = 3600 Seconds
ServerTimeout   = 30 Seconds
SuppTimeout     = 30 Seconds
TxPeriod        = 30 Seconds
Guest-Vlan      = 0

```

This is an example of output from the **show dot1x interface *interface-id*** privileged EXEC command:

```

Switch# show dot1x interface gigabitethernet0/1
Supplicant MAC 00d0.b71b.35de
  AuthSM State      = AUTHENTICATED
  BendSM State      = IDLE
PortStatus          = AUTHORIZED
MaxReq              = 2
HostMode            = Single
Port Control        = Auto
QuietPeriod         = 60 Seconds
Re-authentication   = Disabled
ReAuthPeriod        = 3600 Seconds
ServerTimeout       = 30 Seconds
SuppTimeout         = 30 Seconds
TxPeriod            = 30 Seconds
Guest-Vlan          = 0

```

This is an example of output from the **show dot1x statistics interface *interface-id*** command. [Table 2-11](#) describes the fields in the display.

```

Switch# show dot1x statistics interface gigabitethernet0/1
PortStatistics Parameters for Dot1x
-----
TxReqId = 15    TxReq = 0      TxTotal = 15
RxStart = 4     RxLogoff = 0   RxRespId = 1   RxResp = 1
RxInvalid = 0  RxLenErr = 0   RxTotal = 6
RxVersion = 1  LastRxSrcMac 00d0.b71b.35de

```

**Table 2-11** *show dot1x statistics* Field Descriptions

Field	Description
TxReqId	Number of Extensible Authentication Protocol (EAP)-request/identity frames that have been sent.
TxReq	Number of EAP-request frames (other than request/identity frames) that have been sent.
TxTotal	Number of Extensible Authentication Protocol over LAN (EAPOL) frames of any type that have been sent.
RxStart	Number of valid EAPOL-start frames that have been received.
RxLogoff	Number of EAPOL-logoff frames that have been received.
RxRespId	Number of EAP-response/identity frames that have been received.
RxResp	Number of valid EAP-response frames (other than response/identity frames) that have been received.
RxInvalid	Number of EAPOL frames that have been received and have an unrecognized frame type.

**Table 2-11** *show dot1x statistics Field Descriptions (continued)*

Field	Description
RxLenError	Number of EAPOL frames that have been received in which the packet body length field is invalid.
RxTotal	Number of valid EAPOL frames of any type that have been received.
RxVersion	Number of received packets in the IEEE 802.1x Version 1 format.
LastRxSrcMac	Source MAC address carried in the most recently received EAPOL frame.

**Related Commands**

Command	Description
<a href="#">dot1x default</a>	Resets the configurable IEEE 802.1x parameters to their default values.



# show env

Use the **show env** user EXEC command to display alarm contact, fan, temperature, and power information for the switch.

**show env {alarm-contact | all | fan | power | temperature}**

## Syntax Description

<b>alarm-contact</b>	Display alarm contact status.
<b>all</b>	Display fan, temperature, power supply, and alarm status.
<b>fan</b>	Display the status of the power supply fans. There are two fans in each power supply. If either fan in a power supply fails, the status is reported as FAULTY.
<b>power</b>	Display the switch power-supply status.
<b>temperature</b>	Display the switch temperature status as OK or FAULTY and the temperature thresholds.

## Command Modes

User EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Examples

This is an example of output from the **show env alarm-contact** command:

```
Switch# show env alarm-contact
ALARM CONTACT 1
  Status:      asserted
  Description: main_lab_door
  Severity:    critical
  Trigger:     open
ALARM CONTACT 2
  Status:      asserted
  Description: main_lab_cabinet-1_door
  Severity:    major
  Trigger:     open
ALARM CONTACT 3
  Status:      asserted
  Description: main_lab_supply-room_door
  Severity:    major
  Trigger:     open
ALARM CONTACT 4
  Status:      not asserted
  Description: main_lab_water-level_FLOOD
  Severity:    critical
  Trigger:     closed
```

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

```
Switch# show env all
FAN PS 1 is OK
FAN PS 2 is OK
TEMPERATURE is OK
```

## ■ show env

```

Temperature Value: 23 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 66 Degree Celsius
Red Threshold    : 74 Degree Celsius
POWER SUPPLY 1 is DC OK
POWER SUPPLY 2 is DC OK

```

```

ALARM CONTACT 1 is asserted
ALARM CONTACT 2 is asserted
ALARM CONTACT 3 is asserted
ALARM CONTACT 4 is not asserted

```

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

```

Switch> show env fan
FAN PS 1 is OK
FAN PS 2 is FAULTY

```

This is an example of output from the **show env power** command when both DC inputs are expected but one is missing:

```

Switch# show env power
POWER SUPPLY 1 is DC OK
POWER SUPPLY 2 is DC FAULTY

```

This is an example of output from the **show env power** command when one AC-power supply is present:

```

Switch# show env power
POWER SUPPLY 1 is AC OK
  AC Input   : OK
  Output     : OK
  Fan        : OK
POWER SUPPLY 2 is NOT PRESENT

```

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

```

Switch# show env temperature
TEMPERATURE is OK

```

---

**Related Commands**

Command	Description
<a href="#">alarm-contact</a>	Configures alarm contacts.
<a href="#">power-supply dual</a>	Configures power supply alarms.

# show errdisable detect

Use the **show errdisable detect** user EXEC command to display error-disable detection status.

## show errdisable detect

**Syntax Description** This command has no arguments or keywords.

**Command Modes** User EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** The `Mode` column shows the shutdown mode that was configured for the error-disabled reason:

- `port`—The physical port is error disabled if a violation occurs.
- `vlan`—The virtual port is disabled if a violation occurs.
- `port/vlan`—Some ports are configured for physical port disable, and others are configured for virtual port disable. Enter the **show running config** privileged EXEC command to see the configuration for each port.

A displayed `gbic-invalid` error in the `Reason` column refers to an invalid small form-factor pluggable (SFP) interface.

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

```
Switch> show errdisable detect
ErrDisable Reason  Detection  Mode
-----
arp-inspection     Enabled   port
bpduguard          Enabled   port
channel-misconfig  Enabled   port
community-limit   Enabled   port
dhcp-rate-limit    Enabled   port
dtp-flap           Enabled   port
gbic-invalid        Enabled   port
invalid-policy      Enabled   port
l2ptguard          Enabled   port
link-flap          Enabled   port
link-monitor-fail  Enabled   port
loopback           Enabled   port
lsgroup            Enabled   port
oam-remote-failure Enabled   port
pagp-flap          Enabled   port
psecure-violation  Enabled   port/vlan
security-violatio  Enabled   port
sfp-config-mismatch Enabled   port
storm-control       Enabled   port
udld               Enabled   port
```

## ■ show errdisable detect

```
vmps          Enabled  port
```



### Note

Though visible in the output, the dtp-flap, ilpower, storm-control, and unicast-flood fields are not valid.

### Related Commands

Command	Description
<a href="#">errdisable detect cause</a>	Enables error-disable detection for a specific cause or all causes.
<a href="#">show errdisable flap-values</a>	Displays error condition recognition information.
<a href="#">show errdisable recovery</a>	Displays error-disable recovery timer information.
<a href="#">show interfaces status</a>	Displays interface status or a list of interfaces in an error-disabled state.

# show errdisable flap-values

Use the **show errdisable flap-values** user EXEC command to display conditions that cause an error to be recognized for a cause.

## show errdisable flap-values

**Syntax Description** This command has no arguments or keywords.

**Command Modes** User EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** The *Flaps* column in the display shows how many changes to the state within the specified time interval will cause an error to be detected and a port to be disabled. For example, the display shows that an error will be assumed and the port shut down if three Dynamic Trunking Protocol (DTP)-state (port mode access/trunk) or Port Aggregation Protocol (PAgP) flap changes occur during a 30-second interval, or if 5 link-state (link up/down) changes occur during a 10-second interval.

ErrDisable Reason	Flaps	Time (sec)
pagp-flap	3	30
dtp-flap	3	30
link-flap	5	10



**Note** Although visible in the output display, the switch does not support DTP.

**Examples** This is an example of output from the **show errdisable flap-values** command:

```
Switch> show errdisable flap-values
ErrDisable Reason    Flaps    Time (sec)
-----
pagp-flap            3         30
dtp-flap              3         30
link-flap             5         10
```

## ■ show errdisable flap-values

Related Commands	Command	Description
	<a href="#">errdisable detect cause</a>	Enables error-disable detection for a specific cause or all causes.
	<a href="#">show errdisable detect</a>	Displays error-disable detection status.
	<a href="#">show errdisable recovery</a>	Displays error-disable recovery timer information.
	<a href="#">show interfaces status</a>	Displays interface status or a list of interfaces in error-disabled state.

# show errdisable recovery

Use the **show errdisable recovery** user EXEC command to display the error-disable recovery timer information.

## show errdisable recovery

**Syntax Description** This command has no arguments or keywords.

**Command Modes** User EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

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

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

```
Switch> show errdisable recovery
ErrDisable Reason      Timer Status
-----
udld                   Disabled
bpduguard              Disabled
security-violatio     Disabled
channel-misconfig     Disabled
vmps                   Disabled
pagp-flap              Disabled
dtp-flap               Disabled
l2ptguard              Disabled
link-flap              Enabled
psecure-violation     Disabled
gbic-invalid           Disabled
dhcp-rate-limit       Disabled
unicast-flood         Disabled
storm-control         Disabled
arp-inspection        Disabled
loopback               Disabled
```

## ■ show errdisable recovery

```
Timer interval:300 seconds
Interfaces that will be enabled at the next timeout:
```

Interface	Errdisable reason	Time left(sec)
-----	-----	-----
Gi0/2	link-flap	279



### Note

Though visible in the output, the unicast-flood and DTP fields are not valid.

### Related Commands

Command	Description
<a href="#">errdisable recovery</a>	Configures the recover mechanism variables.
<a href="#">show errdisable detect</a>	Displays error-disabled detection status.
<a href="#">show errdisable flap-values</a>	Displays error condition recognition information.
<a href="#">show interfaces status</a>	Displays interface status or a list of interfaces in error-disabled state.



# show etherchannel

Use the **show etherchannel** user EXEC command to display EtherChannel information for a channel.

```
show etherchannel [channel-group-number {detail | port | port-channel | protocol | summary}]
                 {detail | load-balance | port | port-channel | protocol | summary}
```

## Syntax Description

<i>channel-group-number</i>	(Optional) Number of the channel group. The range is 1 to 48.
<b>detail</b>	Display detailed EtherChannel information.
<b>load-balance</b>	Display the load-balance or frame-distribution scheme among ports in the port channel.
<b>port</b>	Display EtherChannel port information.
<b>port-channel</b>	Display port-channel information.
<b>protocol</b>	Display the protocol that is being used in the EtherChannel.
<b>summary</b>	Display a one-line summary per channel-group.

## Command Modes

User EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

If you do not specify a *channel-group*, 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).



### Note

The switch must be running the metro IP access image to support Layer 3 ports.

**Examples**

This is an example of output from the **show etherchannel 1 detail** command:

```
Switch> show etherchannel 1 detail
Group state = L2
Ports: 2 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol: LACP
          Ports in the group:
          -----
Port: Gi0/1
-----

Port state      = Up Mstr In-Bndl
Channel group = 1          Mode = Active          Gcchange = -
Port-channel   = Po1      GC = -              Pseudo port-channel = Po1
Port index     = 0          Load = 0x00          Protocol = LACP

Flags: S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDU
      A - Device is in active mode.          P - Device is in passive mode.

Local information:

Port      Flags  State      LACP port  Admin  Oper  Port  Port
Gi0/1    SA     bndl      32768      0x0    0x1   0x0   0x3D

Age of the port in the current state: 01d:20h:06m:04s

          Port-channels in the group:
          -----

Port-channel: Po1      (Primary Aggregator)
-----

Age of the Port-channel = 01d:20h:20m:26s
Logical slot/port = 10/1          Number of ports = 2
HotStandBy port = null
Port state      = Port-channel Ag-Inuse
Protocol        = LACP

Ports in the Port-channel:

Index  Load  Port      EC state      No of bits
-----+-----+-----+-----+-----
0      00    Gi0/1     Active        0
0      00    Gi0/2     Active        0

Time since last port bundled: 01d:20h:20m:20s Gi0/2
```

This is an example of output from the **show etherchannel 1 summary** command:

```
Switch> show etherchannel 1 summary
Flags: D - down          P - in port-channel
      I - stand-alone s - suspended
      H - Hot-standby (LACP only)
      R - Layer3          S - Layer2
      u - unsuitable for bundling
      U - in use          f - failed to allocate aggregator
      d - default port

Number of channel-groups in use: 1
Number of aggregators:          1
```

```

Group  Port-channel  Protocol  Ports
-----+-----+-----+-----
1      Po1(SU)          LACP     Gi0/1(P)  Gi0/2(P)

```

This is an example of output from the **show etherchannel 1 port-channel** command:

```

Switch> show etherchannel 1 port-channel
          Port-channels in the group:
          -----
Port-channel: Po1      (Primary Aggregator)

-----

Age of the Port-channel   = 01d:20h:24m:50s
Logical slot/port        = 10/1           Number of ports = 2
HotStandBy port         = null
Port state                = Port-channel Ag-Inuse
Protocol                  = LACP

Ports in the Port-channel:

Index  Load  Port      EC state      No of bits
-----+-----+-----+-----+-----
0      00    Gi0/1     Active        0
 0      00    Gi0/2     Active        0

Time since last port bundled: 01d:20h:24m:44s  Gi0/2

```

This is an example of output from **show etherchannel protocol** command:

```

Switch# show etherchannel protocol
          Channel-group listing:
          -----
Group: 1
-----
Protocol: LACP

Group: 2
-----
Protocol: PAgP

```

#### Related Commands

Command	Description
<a href="#">channel-group</a>	Assigns an Ethernet port to an EtherChannel group.
<a href="#">channel-protocol</a>	Restricts the protocol used on a port to manage channeling.
<a href="#">interface port-channel</a>	Accesses or creates the port channel.

# show ethernet loopback

Use the **show ethernet loopback** privileged EXEC command to display information about per port Ethernet loopbacks configured on the switch or on an interface.

**show ethernet loopback** [*interface-id*]

<b>Syntax Description</b>	<i>interface-id</i>	(Optional) Show loopback information for the specified interface. Only physical interfaces support Ethernet loopback.
---------------------------	---------------------	---

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

<b>Usage Guidelines</b>	If you do not specify an <i>interface-id</i> , all configured loopbacks appear. The switch supports a maximum of two Ethernet loopback configurations.
-------------------------	--

**Examples** This is an example of output from the **show ethernet loopback** command:

```
Switch# show ethernet loopback
=====
Loopback Session 0 : Interface Gi0/3
Status             : configured
MAC Mode           : swap
Time out           : 60
```

This is an example of output with both a port and a VLAN loopback session configured and started.

```
Switch# show ethernet loopback
=====
Loopback Session 0 : Interface Fa0/1
Direction          : facility
Type               : port
Status             : active
MAC Mode           : swap
Time out           : none
=====
Loopback Session 1 : Interface Fa0/2
Direction          : facility
Type               : vlan
Status             : active
MAC Mode           : copy
Vlan               : 3
Time out           : 100
```

Related Commands	Command	Description
	<a href="#">ethernet loopback (interface configuration)</a>	Configures an Ethernet loopback operation on an interface.
	<a href="#">ethernet loopback (privileged EXEC)</a>	Starts or stops the loopback operation.

# show ethernet service evc

Use the **show ethernet service evc** privileged EXEC command to display information about Ethernet virtual connection (EVC) customer-service instances.

**show ethernet service evc** [**id** *evc-id* | **interface** *interface-id*] [**detail**]

Syntax Description	
<b>id</b> <i>evc-id</i>	(Optional) Display EVC information for the specified service. The EVC identifier can be a string of from 1 to 100 characters.
<b>interface</b> <i>interface-id</i>	(Optional) Display EVC information for the specified interface.
<b>detail</b>	(Optional) Display detailed information about EVC service or the specified EVC ID or interface.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Examples** This is an example of output from the **show ethernet service evc** command:

```
Switch# show ethernet service evc
Identifier      Type   Act-UNI-cnt  Status
BLUE           P-P    2             Active
PINK           MP-MP   2             PartiallyActive
PURPLE         P-P    2             Active
BROWN          MP-MP   2             Active
GREEN          P-P    3             Active
YELLOW         MP-MP   2             PartiallyActive
BANANAS        P-P    0             InActive
TEST2          P-P    0             NotDefined
ORANGE         P-P    2             Active
TEAL           P-P    0             InActive
```

Related Commands	Command	Description
	<b>ethernet evc</b> <i>evc-id</i>	Defines an EVC and enters EVC configuration mode.

# show ethernet service instance

Use the **show ethernet service instance** privileged EXEC command to display information about Ethernet customer-service instances.

**show ethernet service instance** [*id id*] [*interface interface-id*] [*detail*]

Syntax Description		
<b>id</b> <i>id</i>	(Optional) Display information for the specified service-instance identifier, a per-interface service identifier that does not map to a VLAN. The range is 1 to 4294967295.	
<b>interface</b> <i>interface-id</i>	(Optional) Display service-instance information for the specified interface.	
<b>detail</b>	(Optional) Display detailed information about service instances or the specified service-instance ID or interface.	

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Examples** This is an example of output from the **show ethernet service instance** command:

```
Switch# show ethernet service instance
Identifier Interface          CE-Vlans
222      FastEthernet0/1          untagged,1-4094
10       FastEthernet0/2
222      FastEthernet0/2          200
333      FastEthernet0/2          default
10       FastEthernet0/3          300
11       FastEthernet0/3
10       FastEthernet0/4          300
10       FastEthernet0/6          untagged,1-4094
10       FastEthernet0/7          untagged,1-4094
10       FastEthernet0/8          untagged,1-4094
10       FastEthernet0/9          untagged
20       FastEthernet0/9
222      FastEthernet0/11         300-350,900-999
333      FastEthernet0/11         100-200,1000,1999-4094
222      FastEthernet0/12         20
333      FastEthernet0/12         10
10       FastEthernet0/13         10
20       FastEthernet0/13         20
30       FastEthernet0/13         30
200      FastEthernet0/13         222
200      FastEthernet0/14         200,222
300      FastEthernet0/14         333
555      FastEthernet0/14         555
```

■ show ethernet service instance

Related Commands	Command	Description
	<code>service instance <i>id</i> ethernet</code>	Defines an Ethernet service instance and enters Ethernet service configuration mode.



# show ethernet service interface

Use the **show ethernet service interface** privileged EXEC command to display interface-based information about Ethernet customer-service instances for all interfaces or a specified interface.

**show ethernet service interface** [*interface-id*] [**detail**]

Syntax Description	
<i>interface-id</i>	(Optional) Display service-instance information for the specified interface.
<b>detail</b>	(Optional) Display detailed information about service instances on all interfaces or the specified interface.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

## Examples

These are examples of outputs from the **show ethernet service interface** commands:

```
Switch# show ethernet service interface gigabitethernet0/1
Interface      Identifier
GigabitEthernet0/1 PE2-G101
```

```
Switch# show ethernet service interface detail
Interface: FastEthernet0/1
ID:
CE-VLANS:
EVC Map Type: Bundling-Multiplexing
Interface: FastEthernet0/2
ID:
CE-VLANS:
EVC Map Type: Bundling-Multiplexing
Interface: FastEthernet0/3
ID:
CE-VLANS:
EVC Map Type: Bundling-Multiplexing
```

<output truncated>

```
Interface: GigabitEthernet0/1
ID: PE2-G101
CE-VLANS: 10,20,30
EVC Map Type: Bundling-Multiplexing
Associated EVCs:
EVC-ID CE-VLAN
WHITE 30
RED 20
BLUE 10
Associated Service Instances:
Service-Instance-ID CE-VLAN
10 10
20 20
30 30
```

■ show ethernet service interface

Related Commands	Command	Description
	<code>service instance <i>id</i> ethernet</code>	Defines an Ethernet service instance and enters Ethernet service configuration mode from interface configuration mode.

# show flowcontrol

Use the **show flowcontrol** user EXEC command to display the flow control status and statistics.

**show flowcontrol** [**interface** *interface-id* | **module** *number*]

Syntax Description	Parameter	Description
	<b>interface</b> <i>interface-id</i>	(Optional) Display the flow control status and statistics for a specific interface.
	<b>module</b> <i>number</i>	(Optional) Display the flow control status and statistics for all interfaces on the switch. The only valid module number is 1. This option is not available if you have entered a specific interface ID.

**Command Modes** User EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** Use this command to display the flow control status and statistics on the switch or for a specific interface. Use the **show flowcontrol** command to display information about all the switch interfaces. The output from the **show flowcontrol** command is the same as the output from the **show flowcontrol module number** command. Use the **show flowcontrol interface interface-id** command to display information about a specific interface.

**Examples** This is an example of output from the **show flowcontrol** command.

```
Switch> show flowcontrol
Port      Send FlowControl  Receive FlowControl  RxPause TxPause
         admin   oper    admin   oper
-----
Gi0/1     Unsupp.  Unsupp.  off     off     0       0
Gi0/2     desired  off      off     off     0       0
Gi0/3     desired  off      off     off     0       0
<output truncated>
```

## show flowcontrol

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

```
Switch> show flowcontrol interface gigabitethernet0/2
Port          Send FlowControl  Receive FlowControl  RxPause TxPause
              admin    oper      admin    oper
-----
Gi0/2        desired off      off      off      0      0
```

### Related Commands

Command	Description
<a href="#">flowcontrol</a>	Sets the receive flow-control state for an interface.

# show idprom

Use the **show idprom** user EXEC command to display the IDPROM information for a Gigabit Ethernet interface.

**show idprom** {**interface** *interface-id*} [**detail**]

Syntax Description	interface <i>interface-id</i>	Display the IDPROM information for the specified Gigabit Ethernet interface.
	<b>detail</b>	(Optional) Display detailed IDPROM information.

**Command Modes** User EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** This command applies only to Gigabit Ethernet interfaces and displays information about SFPs inserted in the SFP module slot.

**Examples** This is an example of output from the **show idprom interface** command for a Gigabit Ethernet interface:

```
Switch# show idprom interface gigabitethernet0/1
General SFP Information
-----
Identifier           : 0x03
Connector            : 0x07
Transceiver          : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
Encoding              : 0x02
BR_Nominal           : 0x01
Vendor Name           : CISCO-NEC
Vendor Part Number    : OD-BP1511-23SL2
Vendor Revision       : 0x30 0x30 0x30 0x31
Vendor Serial Number  : NEC08440067
-----
```

## show idprom

```

Other Information
-----
Port asic num       : 0
Port asic port num  : 0
XCVR init completed : 1
Embedded PHY        : not present
SFP presence index  : 0
SFP iter cnt        : 697918

SFP failed oper flag : 0x0
IIC error cnt       : 0
IIC error dsb cnt   : 0
IIC max sts cnt     : 4
Chk for link status : 1
Link Status         : 1
Link Status Media   : 1
Preferred media     : 0
Resolved Media      : 1
Config Media        : 1
Access Count        : 0
Access Count Max    : 2
Port Rx Loss        : no
Port Tx Fault       : no
Port Tx Disable     : no

Sfp selection asic reg map
-----
stbi                : 0x00
sfpControl           : 0x4C
Regs Loc            : 0xF0000000

-----

Page 0 Registers
-----
0000: 1140 Control Register           : 0001 0001 0100 0000
0001: 6149 Control STATUS             : 0110 0001 0100 1001
0002: 0141 Phy ID 1                   : 0000 0001 0100 0001
0003: 0C92 Phy ID 2                   : 0000 1100 1001 0010
0004: 01E1 Auto-Negotiation Advertisement : 0000 0001 1110 0001
0005: 0000 Auto-Negotiation Link Partner : 0000 0000 0000 0000
0006: 0004 Auto-Negotiation Expansion Reg : 0000 0000 0000 0100
0007: 2001 Next Page Transmit Register  : 0010 0000 0000 0001
0008: 0000 Link Partner Next page Register : 0000 0000 0000 0000
0009: 0F00 1000BASE-T Control Register   : 0000 1111 0000 0000
000A: 0000 1000BASE-T Status Register    : 0000 0000 0000 0000
000F: 0000 Extended Status Register     : 0000 0000 0000 0000
0010: 6028 PHY Specific Control Register : 0110 0000 0010 1000
0011: 6CC8 PHY Specific Status Register  : 0110 1100 1100 1000
0012: 0000 Interrupt Enable Register     : 0000 0000 0000 0000
0013: 0700 PHY Specific Status Register2 : 0000 0111 0000 0000
0015: 01C0 Receive Error Counter         : 0000 0001 1100 0000

0016: 0000 Page Address Register         : 0000 0000 0000 0000
001A: 8040 PHY Specific Control Register2 : 1000 0000 0100 0000

```

## Related Commands

Command	Description
<a href="#">show controllers ethernet-controller</a>	Displays per-interface send and receive statistics read from the hardware, interface internal registers, or port ASIC information.

# show interfaces

Use the **show interfaces** privileged EXEC command to display the administrative and operational status of all interfaces or a specified interface.

```
show interfaces [interface-id [mtu] | vlan vlan-id] [accounting | capabilities [module number] |
counters | description | etherchannel | flowcontrol | private-vlan mapping | rep | stats |
status [err-disabled] | switchport [backup | module number] | transceivers | trunk]
```

Syntax	Description
<i>interface-id</i>	(Optional) Valid interfaces include physical ports (including type, module, and port number) and port channels. The port-channel range is 1 to 48.
<b>mtu</b>	(Optional) Display the maximum transmission unit (MTU) size set on the interface.
<b>vlan</b> <i>vlan-id</i>	(Optional) VLAN identification. The range is 1 to 4094.
<b>accounting</b>	(Optional) Display accounting information on the interface, including active protocols and input and output packets and octets.
<b>capabilities</b>	(Optional) Display the capabilities of all interfaces or the specified interface, including the features and options that you can configure on the interface. Though visible in the command line help, this option is not available for VLAN IDs.
<b>module</b> <i>number</i>	(Optional) Display <b>capabilities</b> , <b>switchport</b> configuration, or <b>transceiver</b> characteristics (depending on preceding keyword) of all interfaces on the switch. The only valid module number is 1. This option is not available if you have entered a specific interface ID.
<b>counters</b>	(Optional) See the <a href="#">show interfaces counters</a> command.
<b>description</b>	(Optional) Display the administrative status and description set for an interface.
<b>etherchannel</b>	(Optional) Display interface EtherChannel information.
<b>flowcontrol</b>	(Optional) Display interface flowcontrol information
<b>private-vlan mapping</b>	(Optional) Display private-VLAN mapping information for the VLAN switch virtual interfaces (SVIs) and private VLAN promiscuous ports. A promiscuous port must be a network node interface (NNI). This keyword is visible only when the switch is running the metro access or metro IP access image.
<b>rep</b>	(Optional) See the <a href="#">show interfaces rep</a> command.
<b>stats</b>	(Optional) Display the input and output packets by switching path for the interface.
<b>status</b>	(Optional) Display the status of the interface. A status of <i>unsupported</i> in the Type field means that a non-Cisco small form-factor pluggable (SFP) module is inserted in the module slot.
<b>err-disabled</b>	(Optional) Display interfaces in error-disabled state.
<b>switchport</b>	(Optional) Display the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
<b>backup</b>	(Optional) Display Flex Link backup interface configuration and status for the specified interface or all interfaces on the switch. This keyword is visible only when the switch is running the metro access or metro IP access image.
<b>transceivers</b>	(Optional) See the <a href="#">show interfaces transceivers</a> command.
<b>trunk</b>	Display 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 **rb**, **fair-queue**, **irb**, **mac-accounting**, **precedence**, **pruning random-detect**, **rate-limit**, and **shape** keywords are not supported.

**Command Modes**

Privileged EXEC

**Command History**

Release	Modification
12.2(44)EY	This command was introduced.

**Usage Guidelines**

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

- Use the **show interface capabilities module 1** to display the capabilities of all interfaces on the switch. Entering any other number is invalid.
- Use the **show interfaces interface-id capabilities** to display the capabilities of the specified interface.
- Use the **show interfaces capabilities** (with no module number or interface ID) to display the capabilities of all interfaces on the switch.
- Use the **show interface switchport module 1** to display the switch port characteristics of all interfaces on the switch. Entering any other number is invalid.

**Examples**

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

```
Switch# show interfaces gigabitethernet0/2
GigabitEthernet0/2 is down, line protocol is down
  Hardware is Gigabit Ethernet, address is 0009.43a7.d085 (bia 0009.43a7.d085)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00 Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    2 packets input, 1040 bytes, 0 no buffer
    Received 0 broadcasts, 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
    4 packets output, 1040 bytes, 0 underruns
    0 output errors, 0 collisions, 3 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 PAUSE output
    0 output buffer failures, 0 output buffers swapped out
```

This is an example of output from the **show interfaces accounting** command.



```

Switch# show interfaces accounting
Vlan1
          Protocol    Pkts In   Chars In   Pkts Out   Chars Out
          IP          1094395   131900022  559555     84077157
          Spanning Tree 283896   17033760   42         2520
          ARP         63738    3825680    231        13860
Interface Vlan2 is disabled
Vlan7
          Protocol    Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.
Vlan31
          Protocol    Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.

GigabitEthernet0/1
          Protocol    Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.
GigabitEthernet0/2
          Protocol    Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.

<output truncated>

```

This is an example of output from the **show interfaces capabilities** command for an interface.

```

Switch# show interfaces gigabitethernet0/2 capabilities
GigabitEthernet0/2
  Model:                modell-ic
  Type:                 10/100/1000BaseTX SFP
  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-(4q2t)
  CoS rewrite:          yes
  ToS rewrite:          yes
  UDLD:                 yes
  SPAN:                 source/destination
  PortSecure:           yes
  Dot1x:                yes

```

This is an example of output from the **show interfaces interface description** command when the interface has been described as *Connects to Marketing* by using the **description** interface configuration command.

```

Switch# show interfaces gigabitethernet0/2 description
Interface Status      Protocol Description
Gi0/2                 up          down    Connects to Marketing

```

This is an example of output from the **show interfaces etherchannel** command when port channels are configured on the switch:

```

Switch# show interfaces etherchannel
----
Port-channel1:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port        = 10/1           Number of ports = 0
GC                        = 0x00000000    HotStandBy port = null
Port state                = Port-channel Ag-Not-Inuse

```

```
Port-channel2:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port        = 10/2           Number of ports = 0
GC                        = 0x00000000    HotStandBy port = null
Port state                = Port-channel Ag-Not-Inuse
```

```
Port-channel3:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port        = 10/3           Number of ports = 0
GC                        = 0x00000000    HotStandBy port = null
Port state                = Port-channel Ag-Not-Inuse
```

This is an example of output from the **show interfaces private-vlan mapping** command when the private-VLAN primary VLAN is VLAN 10 and the secondary VLANs are VLANs 501 and 502:

```
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type
-----
vlan10    501        isolated
vlan10    502        community
```

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

```
Switch# show interfaces vlan 1 stats
Switching path   Pkts In   Chars In   Pkts Out   Chars Out
Processor        1165354  136205310  570800     91731594
Route cache      0         0           0           0
Total            1165354  136205310  570800     91731594
```

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

```
Switch# show interfaces status
Port   Name           Status      Vlan      Duplex  Speed Type
Fa0/1  Fa0/1          connected   1         a-full  a-100 10/100BaseTX
Fa0/2  Fa0/2          connected   1         a-full  a-100 10/100BaseTX
Fa0/3  Fa0/3          notconnect  1         auto    auto  10/100BaseTX
Fa0/4  Fa0/4          disabled    1         auto    auto  10/100BaseTX
Fa0/5  Fa0/5          disabled    1         auto    auto  10/100BaseTX
Fa0/6  Fa0/6          disabled    1         auto    auto  10/100BaseTX
Fa0/7  Fa0/7          disabled    1         auto    auto  10/100BaseTX
Fa0/8  Fa0/8          disabled    1         auto    auto  10/100BaseTX
Fa0/9  Fa0/9          disabled    1         auto    auto  10/100BaseTX
Fa0/10 Fa0/10         disabled    1         auto    auto  10/100BaseTX
Fa0/11 Fa0/11         disabled    1         auto    auto  10/100BaseTX
Fa0/12 Fa0/12         disabled    1         auto    auto  10/100BaseTX
Fa0/13 Fa0/13         disabled    1         auto    auto  10/100BaseTX
Fa0/14 Fa0/14         disabled    1         auto    auto  10/100BaseTX
Fa0/15 Fa0/15         disabled    1         auto    auto  10/100BaseTX
Fa0/16 Fa0/16         disabled    1         auto    auto  10/100BaseTX
Fa0/17 Fa0/17         disabled    1         auto    auto  10/100BaseTX
Fa0/18 Fa0/18         disabled    1         auto    auto  10/100BaseTX
Fa0/19 Fa0/19         disabled    1         auto    auto  10/100BaseTX
Fa0/20 Fa0/20         disabled    1         auto    auto  10/100BaseTX
Fa0/21 Fa0/21         disabled    1         auto    auto  10/100BaseTX
Fa0/22 Fa0/22         disabled    1         auto    auto  10/100BaseTX
Fa0/23 Fa0/23         disabled    1         auto    auto  10/100BaseTX
Fa0/24 Fa0/24         disabled    1         auto    auto  10/100BaseTX
Gi0/1  Gi0/1          notconnect  1         auto    auto  10/100/1000Ba
seTX SFP
Gi0/2  Gi0/2          connected   vl-err-dis a-full a-1000 10/100/1000BaseTX
```

These are examples of output from the **show interfaces status** command for a specific interface when private VLANs are configured. Port 22 is configured as a private-VLAN host port. It is associated with primary VLAN 20 and secondary VLAN 25.

```
Switch# show interfaces fastethernet0/22 status
Port      Name      Status      Vlan      Duplex  Speed  Type
Fa0/22              connected   20,25     a-full  a-100  10/100BaseTX
```

In this example, port 2 is configured as a private-VLAN promiscuous port. The display shows only the primary VLAN 20.

```
Switch# show interfaces gigabitethernet0/2 status
Port      Name      Status      Vlan      Duplex  Speed  Type
Gi0/2               connected   20        a-full  a-100  10/100/1000BaseTX
```

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

```
Switch# show interfaces gigabitethernet0/2 status err-disabled
Port      Name      Status      Reason      Err-disabled Vlans
Gi0/2               connected   elmi evc down  1,200
```

This is an example of output from the **show interfaces switchport** command for a single port. [Table 2-12](#) describes the fields in the display.


**Note**

Private VLAN trunks are not supported in this release, so those fields are not applicable.

```
Switch# show interfaces gigabitethernet0/1 switchport
Name: Gi0/1
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
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 private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Capture Mode Disabled
Capture VLANs Allowed: ALL

Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

```
Administrative Native VLAN tagging: enabled
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 private VLANs: none
```

```
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

```
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

**Table 2-12** *show interfaces switchport Field Descriptions*

Field	Description
Name	Displays the port name.
Switchport	Displays the administrative and operational status of the port. In this display, the port is in switchport mode.
Administrative Mode	Displays the administrative and operational modes.
Operational Mode	
Administrative Trunking Encapsulation	Displays the administrative and operational encapsulation method and whether trunking negotiation is enabled.
Negotiation of Trunking	
Access Mode VLAN	Displays the VLAN ID to which the port is configured.
Trunking Native Mode VLAN	Lists the VLAN ID of the trunk that is in native mode.
Administrative Native VLAN tagging	Displays whether or not VLAN tagging is enabled.
Administrative private-vlan host-association	Displays the administrative VLAN association for private-VLAN host ports.
Administrative private-vlan mapping	Displays the administrative VLAN mapping for private-VLAN promiscuous ports.
Operational private-vlan	Displays the operational private-VLAN status.
Trunking VLANs enabled	Lists the active VLANs on the trunk.
Capture VLANs allowed	Lists the allowed VLANs on the trunk.
Unknown unicast blocked	Displays whether or not unknown multicast and unknown unicast traffic is blocked on the interface.
Unknown multicast blocked	

This is an example of output from the **show interfaces switchport** command for a port configured as a private VLAN promiscuous port. The primary VLAN 20 is mapped to secondary VLANs 25, 30 and 35:

```
Switch# show interface gigabitEthernet0/2 switchport
Name: Gi0/2
Switchport: Enabled
Administrative Mode: private-vlan promiscuous
Operational Mode: private-vlan promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Administrative private-vlan host-association: none
Administrative private-vlan mapping: 20 (VLAN0020) 25 (VLAN0025) 30 (VLAN0030) 35
(VLAN0035)
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 private VLANs: none
Operational private-vlan:
20 (VLAN0020) 25 (VLAN0025)
30 (VLAN0030)
35 (VLAN0035)

<output truncated>
```

This is an example of out put from the **show interfaces switchport backup** command when a Flex Link interface goes down (LINK\_DOWN), and VLANs preferred on this interface are moved to the peer interface of the Flex Link pair. In this example, if interface Gi0/6 goes down, Gi0/8 carries all VLANs of the Flex Link pair.

```
Switch#show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface      Backup Interface      State
-----
GigabitEthernet2/0/6  GigabitEthernet0/8   Active Down/Backup Up

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

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

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

When both interfaces are up, G/0/8 forwards traffic for VLANs 60, 100 to 120, and Gi0/6 will forward traffic for VLANs 1 to 50.

```
Switch#show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface      Backup Interface      State
-----
GigabitEthernet0/6    GigabitEthernet2/0/8  Active Up/Backup Up

Vlans on Interface Gi 0/6: 1-50
Vlans on Interface Gi 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 Gi0/6 goes down, Gi0/8 carries all VLANs of the Flex Link pair.

```
Switch#show interfaces switchport backup
Switch Backup Interface Pairs:
```

```
Active Interface      Backup Interface      State
-----
GigabitEthernet0/6   GigabitEthernet0/8   Active Down/Backup Up
```

```
Vlans on Interface Gi 0/6:
Vlans on Interface Gi 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 Gi0/6 comes up, then VLANs preferred on this interface are blocked on the peer interface Gi0/8 and forwarded on Gi0/6.

```
Switch#show interfaces switchport backup
Switch Backup Interface Pairs:
```

```
Active Interface      Backup Interface      State
-----
GigabitEthernet20/6   GigabitEthernet0/8   Active Up/Backup Up
```

```
Vlans on Interface Gi 0/6: 1-50
Vlans on Interface Gi 0/8: 60, 100-120
```

This is an example of output from the **show interfaces interface-id trunk** command. It displays trunking information for the port.

```
Switch# show interfaces gigabitethernet0/1 trunk
Port      Mode      Encapsulation  Status      Native vlan
Gi0/1     auto      negotiate      trunking    1

Port      Vlans allowed on trunk
Gi0/1     1-4094

Port      Vlans allowed and active in management domain
Gi0/1     1-4

Port      Vlans in spanning tree forwarding state and not pruned
Gi0/1     1-4
```

## Related Commands

Command	Description
<a href="#">switchport access vlan</a>	Configures a port as a static-access or a dynamic-access port.
<a href="#">switchport block</a>	Blocks unknown unicast or multicast traffic on an interface.
<a href="#">switchport backup interface</a>	Configures Flex Links, a pair of Layer 2 interfaces that provide mutual backup.
<a href="#">switchport mode</a>	Configures the VLAN membership mode of a port.
<a href="#">switchport mode private-vlan</a>	Configures a port as a private-VLAN host or a promiscuous port.
<a href="#">switchport private-vlan</a>	Defines private-VLAN association for a host port or private-VLAN mapping for a promiscuous port.

# show interfaces counters

Use the **show interfaces counters** privileged EXEC command to display various counters for the switch or for a specific interface.

**show interfaces** [*interface-id* | **vlan** *vlan-id*] **counters** [**errors** | **trunk**] [**module** *switch-number*] | **etherchannel** | **protocol status**]

Syntax Description		
<i>interface-id</i>	(Optional) ID of the physical interface, including type, module, and port number.	
<b>errors</b>	(Optional) Display error counters.	
<b>trunk</b>	(Optional) Display trunk counters.	
<b>module</b> <i>switch-number</i>	(Optional) Display counters for the specified switch number. The only available value is 1.	
<b>etherchannel</b>	(Optional) Display EtherChannel counters, including octets, broadcast packets, multicast packets, and unicast packets received and sent.	
<b>protocol status</b>	(Optional) Display status of protocols enabled on interfaces.	



## Note

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

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

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

```
Switch# show interfaces counters
Port          InOctets    InUcastPkts  InMcastPkts  InBcastPkts
Fa0/1         0           0            0            0
Fa0/2         0           0            0            0
<output truncated>
```

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

```
Switch# show interfaces counters protocol status
Protocols allocated:
Vlan1: Other, IP
Vlan20: Other, IP, ARP
Vlan30: Other, IP, ARP
Vlan40: Other, IP, ARP
```

## show interfaces counters

```
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
FastEthernet0/1: Other, IP, ARP, CDP
FastEthernet0/2: Other, IP
FastEthernet0/3: Other, IP
FastEthernet0/4: Other, IP
FastEthernet0/5: Other, IP
FastEthernet0/6: Other, IP
FastEthernet0/7: Other, IP
FastEthernet0/8: Other, IP
FastEthernet0/9: Other, IP
FastEthernet0/10: Other, IP, CDP
```

<output truncated>

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

```
Switch# show interfaces counters trunk
Port      TrunkFramesTx  TrunkFramesRx  WrongEncap
Gi0/1          0              0              0
Gi0/2          0              0              0
Gi0/3         80678          4155           0
Gi0/4         82320          126            0
Gi0/5          0              0              0
```

<output truncated>

### Related Commands

Command	Description
<a href="#">show interfaces</a>	Displays additional interface characteristics.



# show interfaces rep

Use the **show interfaces rep** User EXEC command to display Resilient Ethernet Protocol (REP) configuration and status for a specified interface or for all interfaces.

**show interfaces** [*interface-id*] **rep** [**detail**]

Syntax Description	
<i>interface-id</i>	(Optional) Display REP configuration and status for a specified physical interface or port channel ID.
<b>detail</b>	(Optional) Display detailed REP configuration and status information.

**Command Modes** User EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

## Usage Guidelines

In the output for the **show interface rep** [**detail**] command, in addition to an *Open*, *Fail*, or *AP* (alternate port) state, the Port Role might show as *Fail Logical Open* (*FailLogOpen*) or *Fail No Ext Neighbor* (*FailNoNbr*). These states indicate that the port is physically up, but REP is not configured on the neighboring port. In this case, one port goes into a forwarding state for the data path to help maintain connectivity during configuration. The Port Role for this port shows as *Fail Logical Open*; the port forwards all data traffic on all VLANs. The other failed Port Role shows as *Fail No Ext Neighbor*; this port blocks traffic for all VLANs.

When the external neighbors for the failed ports are configured, the failed ports go through the alternate port state transitions and eventually go to an *Open* state or remain as the alternate port, based on the alternate port election mechanism.

In the **show interfaces rep** command output, ports configured as edge no-neighbors are designated with an asterisk (\*) in front of *Primary Edge* or *Secondary Edge*. In the output of the **show interfaces rep detail** command, *No-Neighbor* is spelled out.

The output of this command is also included in the **show tech-support** privileged EXEC command output.

**Examples**

This is sample output from the **show interface rep** command:

```
Switch # show interface rep
Interface          Seg-id  Type          LinkOp  Role
-----
GigabitEthernet 0/1      1      Primary Edge  TWO_WAY  Open
GigabitEthernet 0/2      1      Edge          TWO_WAY  Open
FastEthernet 0/4        2                      INIT_DOWN Fail
```

This is sample output from the **show interface rep** command when the edge port is configured to have no REP neighbor. Note the asterisk (\*) next to *Primary Edge*.

```
Switch# show interface rep
Interface          Seg-id  Type          LinkOp  Role
-----
GigabitEthernet0/1      2                      TWO_WAY  Open
GigabitEthernet0/2      2      Primary Edge* TWO_WAY  Open
```

This is sample output from the **show interface rep** command when external neighbors are not configured:

```
Switch # show interface rep
Interface          Seg-id  Type          LinkOp  Role
-----
GigabitEthernet0/1      1                      NO_NEIGHBOR FailNoNbr
GigabitEthernet0/2      2                      NO_NEIGHBOR FailLogOpen
```

This is sample output from the **show interface rep detail** command for a specified interface:

```
Switch # show interface gigabitethernet0/2 rep detail
GigabitEthernet0/2  REP enabled
Segment-id: 1 (Segment)
PortID: 00030019E85BDD00
Preferred flag: No
Operational Link Status: INIT_DOWN
Current Key: 00000000000000000000
Port Role: Fail
Blocked VLAN: 1-4094
Admin-vlan: 1
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
Configured Load-balancing Block Port: 1234567890123456
Configured Load-balancing Block VLAN: 1-4094
STCN Propagate to: none
LSL PDU rx: 0, tx: 0
HFL PDU rx: 0, tx: 0
BPA TLV rx: 0, tx: 0
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 0, tx: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 0, tx: 0
```

**Related Commands**

Command	Description
<a href="#">rep segment</a>	Enables REP on an interface and assigns a segment ID. This command is also used to configure a port as an edge port, a primary edge port, or a preferred port.
<a href="#">show rep topology [detail]</a>	Displays information about all ports in the segment, including which one was configured and selected as the primary edge port.

# show interfaces transceivers

Use the **show interfaces transceivers** privileged EXEC command to display the physical properties of a small form-factor pluggable (SFP) module interface.

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

Syntax Description	
<i>interface-id</i>	(Optional) Display configuration and status for a specified physical interface.
<b>detail</b>	(Optional) Display calibration properties, including high and low numbers and any alarm information for any Digital Optical Monitoring (DoM)-capable transceiver if one is installed in the switch.
<b>supported-list</b>	(Optional) List all supported DoM transceivers.
<b>threshold-table</b>	(Optional) Display alarm and warning threshold table.  <b>Note</b> This keyword displays the thresholds that are programmed into SFP hardware and are not those used to determine when to send alarms or traps. To view those thresholds, enter the <b>show interfaces transceiver detail</b> command.
<b>module number</b>	(Optional) Limit display to interfaces on module on the switch. The range is 1 to 9. This option is not available if you entered a specific interface ID.
<b>properties</b>	(Optional) Display speed, duplex, and inline power settings on an interface.
<b>threshold-table</b>	(Optional) Display alarm and warning threshold table

**Command Modes** User EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** The threshold values shown in the outputs from the **show interfaces transceiver threshold-table** and the **show interfaces transceiver detail** are not the same. The thresholds shown in the output from the **show interfaces transceiver threshold-table** command are hard-coded in Cisco IOS, but are not supported.

The thresholds shown in the output from the **show interfaces transceiver detail** command are read from the SFP EEPROM and are supported. You should always use the **show interfaces transceiver detail** command to view transceiver thresholds.

The DOM threshold provides a mechanism to send traps when parameters from the EEPROM exceed the thresholds. The firmware reads real-time values, including temperature, voltage, transmitted power and received power, from the SFP EEPROM and compares them against product alarm and warning thresholds. When transceiver traps are enabled, a trap is sent every 10 minutes when thresholds are exceeded.

The reading of entSensorThresholdTable and SNMP notification upon threshold violations in CISCO-ENTITY-SENSOR-MIB is supported only in Cisco IOS Release 12.2(52)SE and later.

**Examples**

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

```
Switch# show interfaces gigabitethernet0/1 transceiver properties
Name : Gi0/1
Administrative Speed: auto
Operational Speed: auto
Administrative Duplex: auto
Administrative Power Inline: enable
Operational Duplex: auto
Administrative Auto-MDIX: off
Operational Auto-MDIX: off
```

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

```
Switch# show interfaces gigabitethernet0/3 transceiver detail
ITU Channel not available (Wavelength not available),
Transceiver is externally calibrated.
mA:milliamperes, dBm:decibels (milliwatts), N/A:not applicable.
++:high alarm, +:high warning, -:low warning, -- :low alarm.
A2D readouts (if they differ), are reported in parentheses.
The threshold values are uncalibrated.
```

Port	Temperature (Celsius)	High Alarm Threshold (Celsius)	High Warn Threshold (Celsius)	Low Warn Threshold (Celsius)	Low Alarm Threshold (Celsius)
Gi0/3	41.5	110.0	103.0	-8.0	-12.0

Port	Voltage (Volts)	High Alarm Threshold (Volts)	High Warn Threshold (Volts)	Low Warn Threshold (Volts)	Low Alarm Threshold (Volts)
Gi0/3	3.20	4.00	3.70	3.00	2.95

Port	Current (milliamperes)	High Alarm Threshold (mA)	High Warn Threshold (mA)	Low Warn Threshold (mA)	Low Alarm Threshold (mA)
Gi0/3	31.0	84.0	70.0	4.0	2.0

<output truncated>

This is an example of output from the **show interfaces transceiver dom-supported-list** command:

```
Switch# show interfaces transceiver dom-supported-list
Transceiver Type          Cisco p/n min version
                           supporting DOM
-----
DWDM GBIC                 ALL
DWDM SFP                  ALL
RX only WDM GBIC         ALL
DWDM XENPAK              ALL
DWDM X2                   ALL
DWDM XFP                  ALL
CWDM GBIC                 NONE
CWDM X2                   ALL
CWDM XFP                  ALL
XENPAK ZR                 ALL
X2 ZR                     ALL
XFP ZR                    ALL
Rx_only_WDM_XENPAK       ALL
XENPAK_ER                 10-1888-03
X2_ER                     ALL
XFP_ER                    ALL
XENPAK_LR                 10-1838-04
```

```
X2_LR          ALL
<output truncated>
```

This is an example of output from the **show interfaces transceiver threshold-table** command. Note that these are thresholds programmed into IOS software, and are NOT used to determine alarms.

Optical Tx	Optical Rx	Temp	Laser Bias	Voltage current	
-----					
DWDM GBIC					
Min1	-0.50	-28.50	0	N/A	4.50
Min2	-0.30	-28.29	5	N/A	4.75
Max2	3.29	-6.69	60	N/A	5.25
Max1	3.50	6.00	70	N/A	5.50
DWDM SFP					
Min1	-0.50	-28.50	0	N/A	3.00
Min2	-0.30	-28.29	5	N/A	3.09
Max2	4.30	-9.50	60	N/A	3.59
Max1	4.50	9.30	70	N/A	3.70
RX only WDM GBIC					
Min1	N/A	-28.50	0	N/A	4.50
Min2	N/A	-28.29	5	N/A	4.75
Max2	N/A	-6.69	60	N/A	5.25
Max1	N/A	6.00	70	N/A	5.50
DWDM XENPAK					
Min1	-1.50	-24.50	0	N/A	N/A
Min2	-1.29	-24.29	5	N/A	N/A
Max2	3.29	-6.69	60	N/A	N/A
Max1	3.50	4.00	70	N/A	N/A
DWDM X2					
Min1	-1.50	-24.50	0	N/A	N/A
Min2	-1.29	-24.29	5	N/A	N/A
Max2	3.29	-6.69	60	N/A	N/A
Max1	3.50	4.00	70	N/A	N/A
DWDM XFP					
Min1	-1.50	-24.50	0	N/A	N/A
Min2	-1.29	-24.29	5	N/A	N/A
Max2	3.29	-6.69	60	N/A	N/A
Max1	3.50	4.00	70	N/A	N/A
CWDM X2					
Min1	N/A	N/A	0	N/A	N/A
Min2	N/A	N/A	0	N/A	N/A
Max2	N/A	N/A	0	N/A	N/A
Max1	N/A	N/A	0	N/A	N/A

#### Related Commands

Command	Description
<a href="#">show interfaces</a>	Displays additional interface characteristics.

# show inventory

Use the **show inventory** user EXEC command to display product identification (PID) information for the hardware.

**show inventory** [*entity-name* | **raw**]

Syntax Description		
	<i>entity-name</i>	(Optional) Display the specified entity. For example, enter the interface (such as gigabitethernet 0/x) into which a small form-factor pluggable (SFP) module is installed to display its identity.
	<b>raw</b>	(Optional) Display every entity in the device.

**Command Modes** User EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** The command is case sensitive. With no arguments, the **show inventory** command produces a compact display of all identifiable entities that have a product identifier. The display shows the entity location (slot identity), entity description, and the unique device identifier (UDI), including PID, version identifier (VID), and serial number (SN) of that entity.

Many legacy SFPs are not programmed with PIDs and VID.s



**Note**

If there is no PID, no output appears when you enter the **show inventory** command.

For the product identifier (PID) and version identifier (VID) of SFP modules, the output of the **show inventory** user EXEC command displays either the correct information or displays *Unspecified* for the PID and nothing for the VID if the SFP module does not have PID and VID information.

**Examples**

This is example output from the **show inventory** command:

```
Switch> show inventory
NAME: "1", DESCR: "model-id"
PID: model-id , VID:Vo1 , SN: FSJC0407839

NAME: "GigabitEthernet0/1", DESCR: "100BaseBX-10U SFP"
PID: , VID: , SN: NEC08440067
NAME: "GigabitEthernet0/2", DESCR: "10/100/1000BaseTX SFP"
PID: , VID: , SN: 00000MTC0839048G
```

# show ip arp inspection

Use the **show ip arp inspection** privileged EXEC command to display the configuration and the operating state of dynamic Address Resolution Protocol (ARP) inspection or the status of this feature for all VLANs or for the specified interface or VLAN.

```
show ip arp inspection [interfaces [interface-id] | log | statistics [vlan vlan-range] | vlan
                        vlan-range]
```

Syntax Description		
<b>interfaces</b> <i>[interface-id]</i>	(Optional) Display the trust state and the rate limit of ARP packets for the specified interface or all interfaces. Valid interfaces include physical ports and port channels.	
<b>log</b>	(Optional) Display the configuration and contents of the dynamic ARP inspection log buffer.	
<b>statistics</b> [vlan <i>vlan-range</i> ]	(Optional) Display statistics for forwarded, dropped, MAC validation failure, IP validation failure, access control list (ACL) permitted and denied, and DHCP permitted and denied packets for the specified VLAN. If no VLANs are specified or if a range is specified, display information only for VLANs with dynamic ARP inspection enabled (active).	You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
<b>vlan</b> <i>vlan-range</i>	(Optional) Display the configuration and the operating state of dynamic ARP inspection for the specified VLAN. If no VLANs are specified or if a range is specified, display information only for VLANs with dynamic ARP inspection enabled (active).	You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Examples** This is an example of output from the **show ip arp inspection** command

```
Switch# show ip arp inspection

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Enabled

  Vlan      Configuration      Operation      ACL Match      Static ACL
  ----      -
  -----
```

## show ip arp inspection

```

      1      Enabled      Active      deny-all      No
Vlan      ACL Logging      DHCP Logging      Probe Logging
----      -
      1      Acl-Match      All      Permit
Vlan      Forwarded      Dropped      DHCP Drops      ACL Drops
----      -
      1      0      0      0      0
Vlan      DHCP Permits      ACL Permits      Probe Permits      Source MAC Failures
----      -
      1      0      0      0      0
Vlan      Dest MAC Failures      IP Validation Failures      Invalid Protocol Data
----      -
      1      0      0      0

```

This is an example of output from the **show ip arp inspection interfaces** command:

```

Switch# show ip arp inspection interfaces
Interface      Trust State      Rate (pps)      Burst Interval
-----
Gi0/1          Untrusted        15              1
Gi0/2          Untrusted        15              1
Gi0/3          Untrusted        15              1

```

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

```

Switch# show ip arp inspection interfaces gigabitethernet0/1
Interface      Trust State      Rate (pps)      Burst Interval
-----
Gi0/1          Untrusted        15              1

```

This is an example of output from the **show ip arp inspection log** command. It shows the contents of the log buffer before the buffers are cleared:

```

Switch# show ip arp inspection log
Total Log Buffer Size : 32
Syslog rate : 10 entries per 300 seconds.
Interface      Vlan      Sender MAC      Sender IP      Num Pkts      Reason      Time
-----
Gi0/1          5         0003.0000.d673  192.2.10.4     5             DHCP Deny   19:39:01 UTC
Mon Mar 1 1993
Gi0/1          5         0001.0000.d774  128.1.9.25     6             DHCP Deny   19:39:02 UTC
Mon Mar 1 1993
Gi0/1          5         0001.c940.1111  10.10.10.1     7             DHCP Deny   19:39:03 UTC
Mon Mar 1 1993
Gi0/1          5         0001.c940.1112  10.10.10.2     8             DHCP Deny   19:39:04 UTC
Mon Mar 1 1993
Gi0/1          5         0001.c940.1114  173.1.1.1     10            DHCP Deny   19:39:06 UTC
Mon Mar 1 1993
Gi0/1          5         0001.c940.1115  173.1.1.2     11            DHCP Deny   19:39:07 UTC
Mon Mar 1 1993
Gi0/1          5         0001.c940.1116  173.1.1.3     12            DHCP Deny   19:39:08 UTC
Mon Mar 1 1993

```

If the log buffer overflows, it means that a log event does not fit into the log buffer, and the display for the **show ip arp inspection log** privileged EXEC command is affected. A -- in the display appears in place of all data except the packet count and the time. No other statistics are provided for the entry. If you see this entry in the display, increase the number of entries in the log buffer, or increase the logging rate in the **ip arp inspection log-buffer** global configuration command.



This is an example of output from the **show ip arp inspection statistics** command. It shows the statistics for packets that have been processed by dynamic ARP inspection for all active VLANs.

```
Switch# show ip arp inspection statistics
Vlan      Forwarded      Dropped      DHCP Drops      ACL Drops
-----
5         3              4618         4605            4
2000     0              0            0               0

Vlan      DHCP Permits    ACL Permits    Source MAC Failures
-----
5         0              12            0
2000     0              0             0

Vlan      Dest MAC Failures  IP Validation Failures
-----
5         0                 9
2000     0                 0
```

For the **show ip arp inspection statistics** command, the switch increments the number of forwarded packets for each ARP request and response packet on a trusted dynamic ARP inspection port. The switch increments the number of ACL or DHCP permitted packets for each packet that is denied by source MAC, destination MAC, or IP validation checks, and the switch increments the appropriate failure count.

This is an example of output from the **show ip arp inspection statistics vlan 5** command. It shows statistics for packets that have been processed by dynamic ARP for VLAN 5.

```
Switch# show ip arp inspection statistics vlan 5
Vlan      Forwarded      Dropped      DHCP Drops      ACL Drops
-----
5         3              4618         4605            4

Vlan      DHCP Permits    ACL Permits    Source MAC Failures
-----
5         0              12            0

Vlan      Dest MAC Failures  IP Validation Failures  Invalid Protocol Data
-----
5         0                 9                       3
```

## ■ show ip arp inspection

This is an example of output from the **show ip arp inspection vlan 5** command. It shows the configuration and the operating state of dynamic ARP inspection for VLAN 5.

```
Switch# show ip arp inspection vlan 5
Source Mac Validation      :Enabled
Destination Mac Validation:Enabled
IP Address Validation      :Enabled

Vlan    Configuration    Operation    ACL Match    Static ACL
----    -
5       Enabled             Active      second       No

Vlan    ACL Logging    DHCP Logging
----    -
5       Acl-Match     All
```

**Related Commands**

Command	Description
<a href="#">arp access-list</a>	Defines an ARP ACL.
<a href="#">clear ip arp inspection log</a>	Clears the dynamic ARP inspection log buffer.
<a href="#">clear ip arp inspection statistics</a>	Clears the dynamic ARP inspection statistics.
<a href="#">ip arp inspection log-buffer</a>	Configures the dynamic ARP inspection logging buffer.
<a href="#">ip arp inspection vlan logging</a>	Controls the type of packets that are logged per VLAN.
<a href="#">show arp access-list</a>	Displays detailed information about ARP access lists.

# show ip dhcp snooping

Use the **show ip dhcp snooping** user EXEC command to display the DHCP snooping configuration.

**show ip dhcp snooping**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** User EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Examples** This is an example of output from the **show ip dhcp snooping** command.

```
Switch> show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
40-42
Insertion of option 82 is enabled
Option 82 on untrusted port is allowed
Verification of hwaddr field is enabled
Interface                Trusted      Rate limit (pps)
-----                -
GigabitEthernet0/1      yes         unlimited
GigabitEthernet0/2      yes         unlimited
```

Related Commands	Command	Description
	<a href="#">show ip dhcp snooping binding</a>	Displays the DHCP snooping binding information.

## show ip dhcp snooping binding

Use the **show ip dhcp snooping binding** user EXEC command to display the DHCP snooping binding database and configuration information for all interfaces on a switch.

```
show ip dhcp snooping binding [ip-address] [mac-address] [interface interface-id] [vlan vlan-id]
```

Syntax Description		
<i>ip-address</i>	(Optional)	Specify the binding entry IP address.
<i>mac-address</i>	(Optional)	Specify the binding entry MAC address.
<b>interface</b> <i>interface-id</i>	(Optional)	Specify the binding input interface.
<b>vlan</b> <i>vlan-id</i>	(Optional)	Specify the binding entry VLAN.

**Command Modes** User EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** The **show ip dhcp snooping binding** command output shows only the dynamically configured bindings. Use the **show ip source binding** privileged EXEC command to display the dynamically and statically configured bindings in the DHCP snooping binding database.

If DHCP snooping is enabled and an interface changes to the down state, the switch does not delete the statically configured bindings.

**Examples** This example shows how to display the DHCP snooping binding entries for a switch:

```
Switch> show ip dhcp snooping binding
-----
MacAddress      IpAddress      Lease(sec)  Type           VLAN  Interface
-----
01:02:03:04:05:06  10.1.2.150    9837        dhcp-snooping  20    GigabitEthernet0/1
00:D0:B7:1B:35:DE  10.1.2.151    237         dhcp-snooping  20    GigabitEthernet0/2
Total number of bindings: 2
```

This example shows how to display the DHCP snooping binding entries for a specific IP address:

```
Switch> show ip dhcp snooping binding 10.1.2.150
-----
MacAddress      IPAddress      Lease(sec)    Type          VLAN    Interface
-----
01:02:03:04:05:06  10.1.2.150    9810         dhcp-snooping  20     GigabitEthernet0/1
Total number of bindings: 1
```

This example shows how to display the DHCP snooping binding entries for a specific MAC address:

```
Switch> show ip dhcp snooping binding 0102.0304.0506
-----
MacAddress      IPAddress      Lease(sec)    Type          VLAN    Interface
-----
01:02:03:04:05:06  10.1.2.150    9788         dhcp-snooping  20     GigabitEthernet0/2
Total number of bindings: 1
```

This example shows how to display the DHCP snooping binding entries on a port:

```
Switch> show ip dhcp snooping binding interface gigabitethernet0/2
-----
MacAddress      IPAddress      Lease(sec)    Type          VLAN    Interface
-----
00:30:94:C2:EF:35  10.1.2.151    290          dhcp-snooping  20     GigabitEthernet0/2
Total number of bindings: 1
```

This example shows how to display the DHCP snooping binding entries on VLAN 20:

```
Switch> show ip dhcp snooping binding vlan 20
-----
MacAddress      IPAddress      Lease(sec)    Type          VLAN    Interface
-----
01:02:03:04:05:06  10.1.2.150    9747         dhcp-snooping  20     GigabitEthernet0/1
00:00:00:00:00:02  10.1.2.151    65          dhcp-snooping  20     GigabitEthernet0/2
Total number of bindings: 2
```

Table 2-13 describes the fields in the `show ip dhcp snooping binding` command output:

**Table 2-13** *show ip dhcp snooping binding Command Output*

Field	Description
MacAddress	Client hardware MAC address
IpAddress	Client IP address assigned from the DHCP server
Lease(sec)	Remaining lease time for the IP address
Type	Binding type
VLAN	VLAN number of the client interface
Interface	Interface that connects to the DHCP client host
Total number of bindings	Total number of bindings configured on the switch
	<b>Note</b> The command output might not show the total number of bindings. For example, if 200 bindings are configured on the switch and you stop the display before all the bindings appear, the total number does not change.

#### Related Commands

Command	Description
<a href="#">ip dhcp snooping binding</a>	Configures the DHCP snooping binding database
<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.

# show ip dhcp snooping database

Use the **show ip dhcp snooping database** user EXEC command to display the status of the DHCP snooping binding database agent.

## show ip dhcp snooping database [detail]

<b>Syntax Description</b>	<b>detail</b> (Optional) Display detailed status and statistics information.				
<b>Command Modes</b>	User EXEC				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(44)EY</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(44)EY	This command was introduced.
Release	Modification				
12.2(44)EY	This command was introduced.				

### Examples

This is an example of output from the **show ip dhcp snooping database** command:

```
Switch> show ip dhcp snooping database
Agent URL :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts      :          0  Startup Failures :          0
Successful Transfers :          0  Failed Transfers :          0
Successful Reads    :          0  Failed Reads    :          0
Successful Writes   :          0  Failed Writes   :          0
Media Failures      :          0
```

This is an example of output from the **show ip dhcp snooping database detail** command:

```
Switch# show ip dhcp snooping database detail
Agent URL : tftp://10.1.1.1/directory/file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 7 (00:00:07)
Abort Timer Expiry : Not Running

Last Succeeded Time : None
Last Failed Time : 17:14:25 UTC Sat Jul 7 2001
Last Failed Reason : Unable to access URL.

Total Attempts      :          21  Startup Failures :          0
Successful Transfers :          0  Failed Transfers :          21
```

```

Successful Reads      :      0   Failed Reads      :      0
Successful Writes    :      0   Failed Writes     :     21
Media Failures       :      0

```

First successful access: Read

```

Last ignored bindings counters :
Binding Collisions   :      0   Expired leases    :      0
Invalid interfaces   :      0   Unsupported vlans :      0
Parse failures       :      0
Last Ignored Time   : None

```

```

Total ignored bindings counters:
Binding Collisions   :      0   Expired leases    :      0
Invalid interfaces   :      0   Unsupported vlans :      0
Parse failures       :      0

```

### Related Commands

Command	Description
<a href="#">ip dhcp snooping</a>	Enables DHCP snooping on a VLAN.
<a href="#">ip dhcp snooping database</a>	Configures the DHCP snooping binding database agent or the binding file.
<a href="#">show ip dhcp snooping</a>	Displays DHCP snooping information.

# show ip dhcp snooping statistics

Use the **show ip dhcp snooping statistics** user EXEC command to display DHCP snooping statistics in summary or detail form.

## show ip dhcp snooping statistics [detail]

<b>Syntax Description</b>	<b>detail</b> (Optional) Display detailed statistics information.
---------------------------	---

<b>Command Modes</b>	User EXEC
----------------------	-----------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

### Examples

This is an example of output from the **show ip dhcp snooping statistics** command:

```
Switch> 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:

```
Switch> 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
```

[Table 2-14](#) shows the DHCP snooping statistics and their descriptions:

**Table 2-14 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.



**Table 2-14 DHCP Snooping Statistics**

<b>DHCP Snooping Statistic</b>	<b>Description</b>
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 <b>no ip dhcp snooping information option allow-untrusted</b> 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 <b>ip dhcp snooping verify mac-address</b> 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.
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.

Table 2-14 DHCP Snooping Statistics

DHCP Snooping Statistic	Description
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 <b>no ip dhcp snooping information option allow-untrusted</b> 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 <b>ip dhcp snooping verify mac-address</b> 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.
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.

**Table 2-14 DHCP Snooping Statistics**

DHCP Snooping Statistic	Description
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 <b>no ip dhcp snooping information option allow-untrusted</b> 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 <b>ip dhcp snooping verify mac-address</b> 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.
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.

**Table 2-14** DHCP Snooping Statistics

DHCP Snooping Statistic	Description
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.

**Related Commands**

Command	Description
<a href="#">clear ip dhcp snooping</a>	Clears the DHCP snooping binding database, the DHCP snooping binding database agent statistics, or the DHCP snooping statistics counters.

# show ip igmp profile

Use the **show ip igmp profile** privileged EXEC command to display all configured Internet Group Management Protocol (IGMP) profiles or a specified IGMP profile.

**show ip igmp profile** [*profile number*]

<b>Syntax Description</b>	<i>profile number</i> (Optional) The IGMP profile number to be displayed. The range is 1 to 4294967295. If no profile number is entered, all IGMP profiles are displayed.
---------------------------	---

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

**Examples** These are examples of output from the **show ip igmp profile** privileged EXEC command, with and without specifying a profile number. If no profile number is entered, the display includes all profiles configured on the switch.

```
Switch# show ip igmp profile 40
IGMP Profile 40
  permit
  range 233.1.1.1 233.255.255.255
```

```
Switch# show ip igmp profile
IGMP Profile 3
  range 230.9.9.0 230.9.9.0
IGMP Profile 4
  permit
  range 229.9.9.0 229.255.255.255
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">ip igmp profile</a>	Configures the specified IGMP profile number.

# show ip igmp snooping

Use the **show ip igmp snooping** user EXEC command to display the Internet Group Management Protocol (IGMP) snooping configuration of the switch or the VLAN.

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

Syntax Description	
<b>groups</b>	(Optional) See the <a href="#">show ip igmp snooping groups</a> command.
<b>mrouter</b>	(Optional) See the <a href="#">show ip igmp snooping mrouter</a> command.
<b>querier</b>	(Optional) See the <a href="#">show ip igmp snooping querier</a> command.
<b>vlan</b> <i>vlan-id</i>	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094 (available only in privileged EXEC mode).

**Command Modes** User EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** Use this command to display snooping configuration for the switch or for a specific VLAN. VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

Although visible in the output display, output lines for source-only learning are not valid.

**Examples** This is an example of output from the **show ip igmp snooping vlan 1** command. It shows snooping characteristics for a specific VLAN.

```
Switch# show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
-----
IGMP snooping                :Enabled
IGMPv3 snooping (minimal)    :Enabled
Report suppression           :Enabled
TCN solicit query            :Disabled
TCN flood query count        :2
Last member query interval   : 100

Vlan 1:
-----
IGMP snooping                :Enabled
Immediate leave               :Disabled
Multicast router learning mode :pim-dvmrp
Source only learning age timer :10
CGMP interoperability mode    :IGMP_ONLY
Last member query interval   : 100
```

**Note**

Source-only learning are not supported, and information appearing for this feature is not valid.

This is an example of output from the **show ip igmp snooping** command. It displays snooping characteristics for all VLANs on the switch.

```
Switch> show ip igmp snooping
Global IGMP Snooping configuration:
-----
IGMP snooping                : Enabled
IGMPv3 snooping (minimal)    : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Last member query interval   : 100

Vlan 1:
-----
IGMP snooping                :Enabled
Immediate leave               :Disabled
Multicast router learning mode :pim-dvmrp
Source only learning age timer :10
CGMP interoperability mode    :IGMP_ONLY
Last member query interval    : 100

Vlan 2:
-----
IGMP snooping                :Enabled
Immediate leave               :Disabled
Multicast router learning mode :pim-dvmrp
Source only learning age timer :10
CGMP interoperability mode    :IGMP_ONLY
Last member query interval    : 333

<output truncated>
```

**Related Commands**

Command	Description
<a href="#">ip igmp snooping</a>	Enables and configures IGMP snooping on the switch or on a VLAN.
<a href="#">show ip igmp snooping mrouter</a>	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN.
<a href="#">show ip igmp snooping querier</a>	Displays the configuration and operation information for the IGMP querier configured on a switch.

# show ip igmp snooping groups

Use the **show ip igmp snooping groups** privileged EXEC command to display the Internet Group Management Protocol (IGMP) snooping multicast table for the switch or the multicast information. Use with the **vlan** keyword to display the multicast table for a specified multicast VLAN or specific multicast information.

```
show ip igmp snooping groups [count | dynamic [count] | user [count]]
```

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

## Syntax Description

<b>count</b>	(Optional) Display the total number of entries for the specified command options instead of the actual entries.
<b>dynamic</b>	(Optional) Display entries learned by IGMP snooping.
<b>user</b>	(Optional) Display only the user-configured multicast entries.
<b>ip_address</b>	(Optional) Display characteristics of the multicast group with the specified group IP address.
<b>vlan-id</b>	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

Use this command to display multicast information or the multicast table.

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



**Examples**

This is an example of output from the **show ip igmp snooping groups** command without any keywords. It displays the multicast table for the switch.

```
Switch# show ip igmp snooping groups
Vlan      Group      Type      Version   Port List
-----
104       224.1.4.2  igmp     v2        Gi0/1, Gi0/2
104       224.1.4.3  igmp     v2        Gi0/1, Gi0/2
```

This is an example of output from the **show ip igmp snooping groups count** command. It displays the total number of multicast groups on the switch.

```
Switch# show ip igmp snooping groups count
Total number of multicast groups: 2
```

This is an example of output from the **show ip igmp snooping groups dynamic** command. It shows only the entries learned by IGMP snooping.

```
Switch# show ip igmp snooping groups vlan 1 dynamic
Vlan      Group      Type      Version   Port List
-----
104       224.1.4.2  igmp     v2        Gi0/1, Fa0/15
104       224.1.4.3  igmp     v2        Gi0/1, Fa0/15
```

This is an example of output from the **show ip igmp snooping groups vlan *vlan-id ip-address*** command. It shows the entries for the group with the specified IP address.

```
Switch# show ip igmp snooping groups vlan 104 224.1.4.2
Vlan      Group      Type      Version   Port List
-----
104       224.1.4.2  igmp     v2        Gi0/1, Fa0/15
```

**Related Commands**

Command	Description
<a href="#">ip igmp snooping</a>	Enables and configures IGMP snooping on the switch or on a VLAN.
<a href="#">show ip igmp snooping</a>	Displays the IGMP snooping configuration of the switch or the VLAN.
<a href="#">show ip igmp snooping mrouter</a>	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN.

## show ip igmp snooping mrouter

Use the **show ip igmp snooping mrouter** privileged EXEC command to display the Internet Group Management Protocol (IGMP) snooping dynamically learned and manually configured multicast router ports for the switch or for the specified multicast VLAN.

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

<b>Syntax Description</b>	<b>vlan <i>vlan-id</i></b> (Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.
---------------------------	--

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

<b>Usage Guidelines</b>	<p>Use this command to display multicast router ports on the switch or for a specific VLAN.</p> <p>VLAN IDs 1002 to 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 <b>show ip igmp snooping mrouter</b> command displays MVR multicast router information and IGMP snooping information.</p>
-------------------------	--

<b>Examples</b>	<p>This is an example of output from the <b>show ip igmp snooping mrouter</b> command. It shows how to display multicast router ports on the switch.</p>
-----------------	--

```
Switch# show ip igmp snooping mrouter
Vlan      ports
----      -
1         Gi0/1(dynamic)
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">ip igmp snooping</a>	Enables and configures IGMP snooping on the switch or a VLAN.
	<a href="#">ip igmp snooping vlan mrouter</a>	Adds a multicast router port to a multicast VLAN.
	<a href="#">show ip igmp snooping</a>	Displays the IGMP snooping configuration of the switch or VLAN.
	<a href="#">show ip igmp snooping groups</a>	Displays IGMP snooping multicast information for the switch or for the specified parameter.

# show ip igmp snooping querier

Use the **show ip igmp snooping querier** user EXEC command to display the IP address and incoming port for the Internet Group Management Protocol (IGMP) query most recently received by the switch.

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

## Syntax Description

<b>vlan</b> <i>vlan-id</i>	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.
<b>detail</b>	(Optional) Display querier information as well as configuration and operational information pertaining to the querier.

## Command Modes

User EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

Use the **show ip igmp snooping querier** command to display the IGMP version and IP address of a detected device (also called a *querier*) that sends IGMP query message. A subnet can have multiple multicast routers but has only one IGMP querier. In a subnet running IGMPv2, one of the multicast routers is elected as the querier. The querier can be a Layer 3 switch.

The **show ip igmp snooping querier** command output also shows the VLAN and interface on which the querier was detected. If the querier is the switch, the output shows the *Port* field as *Router*. If the querier is a router, the output shows the port number on which the querier is learned in the *Port* field.

The **show ip igmp snooping querier detail** user EXEC command is similar to the **show ip igmp snooping querier** command. However, the **show ip igmp snooping querier detail** command **displays the IP address of the most recent device detected by the switch querier along with this additional information:**

- The elected IGMP querier in the VLAN
- The configuration and operational information pertaining to the switch querier (if any) that is configured in the VLAN

**Examples**

This is an example of output from the **show ip igmp snooping querier** command:

```
Switch> show ip igmp snooping querier
Vlan      IP Address      IGMP Version      Port
-----
1         172.20.50.11   v3                 Gi0/1
2         172.20.40.20   v2                 Router
```

This is an example of output from the **show ip igmp snooping querier detail** command:

```
Switch> show ip igmp snooping querier detail

Vlan      IP Address      IGMP Version      Port
-----
1         1.1.1.1         v2                 Fa0/1

Global IGMP switch querier status
-----
admin state           : Enabled
admin version         : 2
source IP address     : 0.0.0.0
query-interval (sec) : 60
max-response-time (sec) : 10
querier-timeout (sec) : 120
tcn query count       : 2
tcn query interval (sec) : 10

Vlan 1: IGMP switch querier status
-----
elected querier is 1.1.1.1      on port Fa0/1
-----
admin state           : Enabled
admin version         : 2
source IP address     : 10.1.1.65
query-interval (sec) : 60
max-response-time (sec) : 10
querier-timeout (sec) : 120
tcn query count       : 2
tcn query interval (sec) : 10
operational state     : Non-Querier
operational version   : 2
tcn query pending count : 0
```

**Related Commands**

Command	Description
<a href="#">ip igmp snooping querier</a>	Enables and configures the IGMP snooping querier on the switch or on a VLAN.
<a href="#">show ip igmp snooping mrouter</a>	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN.

# show ip sla standards

Use the **show ip sla standards** command in user EXEC or privileged EXEC mode to display the Cisco IOS IP Service Level Agreements (SLAs) and Two-Way Active Measurement Protocol (TWAMP) standards implemented on the switch.

## show ip sla standards

**Syntax Description** This command has no arguments or keywords.

**Defaults** Displays the IP SLAs and TWAMP standards implemented on the switch.

**Command Modes** User EXEC

Command History	Release	Modification
	12.2(52)SE	This command was introduced.

**Usage Guidelines** Use the **show ip sla standards** command to display the IP SLAs TWAMP standards implemented on the switch.

**Examples** The following is sample output from the **show ip sla standards** command:

```
Switch> show ip sla standards
Feature                Organization      Standard
TWAMP Server           IETF              draft-ietf-ippm-twamp-06
TWAMP Reflector        IETF              draft-ietf-ippm-twamp-06
```

Related Commands	Command	Description
	<a href="#">show ip sla twamp connection {detail   requests}</a>	Displays IP SLAs TWAMP connections.
	<a href="#">show ip sla twamp session</a>	Displays IP SLAs TWAMP sessions.

# show ip sla twamp connection

Use the **show ip sla twamp connection** command in user EXEC mode to display the current Cisco IOS IP Service Level Agreements (SLAs) Two-Way Active Measurement Protocol (TWAMP) connections.

```
show ip sla twamp connection {detail [source-ip ip-address] | requests}
```

Syntax Description	detail	Display current connection details.
	source-ip ip-address	(Optional) Display connection details from a specific TWAMP connection.
	requests	Display current connection requests.

**Defaults** Displays output for all running IP SLAs TWAMP sessions.

**Command Modes** User EXEC

Command History	Release	Modification
	12.2(52)SE	This command was introduced.

**Usage Guidelines** Use the **detail** keyword to display detailed information for a single IP SLAs TWAMP connection.  
Use the **requests** keyword to display the current IP SLAs TWAMP connection requests.

**Examples** The following is sample output from the **show ip sla twamp connection detail** command:

```
Switch> show ip sla twamp connection detail
Connection Id:          91
  Client IP Address:    172.27.111.225
  Client Port:         43026
  Mode:                Unauthenticated
  Connection State:    Connected
  Control State:       None
  Number of Test Requests - 0:1
```

The following is sample output from the **show ip sla twamp connection requests** command:

```
Switch> show ip sla twamp connection requests
Connection-Id      Client Address    Client Port
          91          172.27.111.225      43026
Total number of current connections: 1
```

**Related Commands**

Command	Description
<a href="#">show ip sla standards</a>	Displays the TWAMP server and reflector standards implemented on the switch.
<a href="#">show ip sla twamp session</a>	Displays IP SLAs TWAMP sessions.

# show ip sla twamp session

Use the **show ip sla twamp session** command in user EXEC mode to display Cisco IOS IP Service Level Agreements (SLAs) Two-Way Active Measurement Protocol (TWAMP) test sessions.

**show ip sla twamp session** [**source-ip** *ip address* | **source-port** *port-number*]

<b>Syntax Description</b>	<b>source-ip</b> <i>ip-address</i>	(Optional) Display results from the TWAMP test session on the specified IP address.
	<b>source-port</b> <i>port-number</i>	(Optional) Display results from the TWAMP test session on the specified port.
<b>Defaults</b>	Displays the IP SLAs TWAMP test sessions and results.	
<b>Command Modes</b>	User EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(52)SE	This command was introduced.
<b>Usage Guidelines</b>	Use the <b>show ip sla twamp session</b> command to display information about IP SLAs TWAMP test sessions.	
<b>Examples</b>	The following is sample output from the <b>show ip sla twamp session</b> command:	
	<pre>Switch&gt; show ip sla twamp session IP SLAs Responder TWAMP is: Enabled Recv Addr: 172.27.117.116 Recv Port: 3619 Sender Addr: 172.27.111.225 Sender Port: 32910 Session Id: 172.27.117.116:533112:9C41EC42 Connection Id: 95</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show ip sla standards</a>	Displays the TWAMP server and reflector standards implemented on the switch.
	<a href="#">show ip sla twamp connection</a> { <b>detail</b>   <b>requests</b> }	Displays IP SLAs TWAMP connections.



# show ip source binding

Use the **show ip source binding** user EXEC command to display the IP source bindings on the switch.

```
show ip source binding [ip-address] [mac-address] [dhcp-snooping | static] [vlan vlan-id]
[interface interface-id]
```

Syntax Description		
<i>ip-address</i>	(Optional)	Display IP source bindings for a specific IP address.
<i>mac-address</i>	(Optional)	Display IP source bindings for a specific MAC address.
<b>dhcp-snooping</b>	(Optional)	Display IP source bindings that were learned by DHCP snooping.
<b>static</b>	(Optional)	Display static IP source bindings.
<b>vlan</b> <i>vlan-id</i>	(Optional)	Display IP source bindings on a specific VLAN.
<b>interface</b> <i>interface-id</i>	(Optional)	Display IP source bindings on a specific interface.

**Command Modes** User EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** The **show ip source binding** command output shows the dynamically and statically configured bindings in the DHCP snooping binding database. Use the **show ip dhcp snooping binding** privileged EXEC command to display only the dynamically configured bindings.

**Examples** This is an example of output from the **show ip source binding** command:

```
Switch> show ip source binding
MacAddress      IpAddress      Lease(sec)  Type           VLAN  Interface
-----
00:00:00:0A:00:0B  11.0.0.1      infinite    static         10    GigabitEthernet0/1
00:00:00:0A:00:0A  11.0.0.2      10000       dhcp-snooping  10    GigabitEthernet0/1
```

Related Commands	Command	Description
	<a href="#">ip dhcp snooping binding</a>	Configures the DHCP snooping binding database.
	<a href="#">ip source binding</a>	Configures static IP source bindings on the switch.

## show ip verify source

Use the **show ip verify source** user EXEC command to display the IP source guard configuration on the switch or on a specific interface.

**show ip verify source** [**interface** *interface-id*]

### Syntax Description

**interface** *interface-id* (Optional) Display IP source guard configuration on a specific interface.

### Command Modes

User EXEC

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Examples

This is an example of output from the **show ip verify source** command:

```
Switch> show ip verify source
Interface  Filter-type  Filter-mode  IP-address      Mac-address      Vlan
-----
fa0/1     ip           active       10.0.0.1        -----
fa0/1     ip           active       deny-all       11-20
fa0/2     ip           inactive-trust-port
fa0/3     ip           inactive-no-snooping-vlan
fa0/4     ip-mac      active       10.0.0.2        aaaa.bbbb.cccc  10
fa0/4     ip-mac      active       11.0.0.1        aaaa.bbbb.cccd  11
fa0/4     ip-mac      active       deny-all       deny-all        12-20
fa0/5     ip-mac      active       10.0.0.3        permit-all      10
fa0/5     ip-mac      active       deny-all       permit-all      11-20
```

In the previous example, this is the IP source guard configuration:

- On the Fast Ethernet 0/1 interface, dynamic host control protocol (DHCP) snooping is enabled on VLANs 10 to 20. For VLAN 10, IP source guard with IP address filtering is configured on the interface, and a binding is on the interface. For VLANs 11 to 20, the second entry shows that a default port access control list (ACL) is applied on the interface for the VLANs on which IP source guard is not configured.
- The Fast Ethernet 0/2 interface is configured as trusted for DHCP snooping.
- On the Fast Ethernet 0/3 interface, DHCP snooping is not enabled on the VLANs to which the interface belongs.
- On the Fast Ethernet 0/4 interface, IP source guard with source IP and MAC address filtering is enabled, and static IP source bindings are configured on VLANs 10 and 11. For VLANs 12 to 20, the default port ACL is applied on the interface for the VLANs on which IP source guard is not configured.
- On the Fast Ethernet 0/5 interface, IP source guard with source IP and MAC address filtering is enabled and configured with a static IP binding, but port security is disabled. The switch cannot filter source MAC addresses.

This is an example of output on an interface on which IP source guard is disabled:

```
Switch> show ip verify source gigabitethernet0/6  
IP source guard is not configured on the interface gi0/6.
```

---

**Related Commands**

Command	Description
<a href="#">ip verify source</a>	Enables IP source guard on an interface.

---

# show ipc

Use the **show ipc** user EXEC command to display Interprocess Communications Protocol (IPC) configuration, status, and statistics.

```
show ipc {mcast {appclass | groups | status} | nodes | ports [open] | queue | rpc | session {all | rx | tx} [verbose] | status [cumulative] | zones}
```

## Syntax Description

<b>mcast {appclass   groups   status}</b>	Display the IPC multicast routing information. The keywords have these meanings: <ul style="list-style-type: none"> <li><b>appclass</b>—Display the IPC multicast application classes.</li> <li><b>groups</b>—Display the IPC multicast groups.</li> <li><b>status</b>—Display the IPC multicast routing status.</li> </ul>
<b>nodes</b>	Display participating nodes.
<b>ports [open]</b>	Display local IPC ports. The keyword has this meaning: <ul style="list-style-type: none"> <li><b>open</b>—(Optional) Display only the open ports.</li> </ul>
<b>queue</b>	Display the contents of the IPC transmission queue.
<b>rpc</b>	Display the IPC remote-procedure statistics.
<b>session {all   rx   tx}</b>	Display the IPC session statistics (available only in privileged EXEC mode). The keywords have these meanings: <ul style="list-style-type: none"> <li><b>all</b>—Display all the session statistics.</li> <li><b>rx</b>—Display the sessions statistics for traffic that the switch receives</li> <li><b>tx</b>—Display the sessions statistics for traffic that the switch forwards.</li> </ul>
<b>verbose</b>	(Optional) Display detailed statistics (available only in privileged EXEC mode).
<b>status [cumulative]</b>	Display the status of the local IPC server. The keyword has this meaning: <ul style="list-style-type: none"> <li><b>cumulative</b>—(Optional) Display the status of the local IPC server since the switch was started or restarted.</li> </ul>
<b>zones</b>	Display participating IPC zones. The switch supports one IPC zone.

## Command Modes

User EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

**Examples**

This example shows how to display the IPC routing status:

```
Switch> show ipc mcast status
                    IPC Mcast Status
                    Tx           Rx
Total Frames                0           0
Total control Frames        0           0
Total Frames dropped        0           0
Total control Frames dropped 0           0
Total Reliable messages     0           0
Total Reliable messages acknowledged 0           0
Total Out of Band Messages  0           0
Total Out of Band messages acknowledged 0           0
Total No Mcast groups      0           0
Total Retries                0 Total Timeouts                0
Total OOB Retries           0 Total OOB Timeouts        0
Total flushes               0 Total No ports            0
```

This example shows how to display the participating nodes:

```
Switch> show ipc nodes
There is 1 node in this IPC realm.
  ID   Type   Name           Last Sent  Last Heard
  10000 Local   IPC Master     0         0
```

This example shows how to display the local IPC ports:

```
Switch> show ipc ports
There are 8 ports defined.
Port ID      Type      Name                                     (current/peak/total)
There are 8 ports defined.
  10000.1    unicast   IPC Master:Zone
  10000.2    unicast   IPC Master:Echo
  10000.3    unicast   IPC Master:Control
  10000.4    unicast   IPC Master:Init
  10000.5    unicast   FIB Master:DFS.process_level.msgs
  10000.6    unicast   FIB Master:DFS.interrupt.msgs
  10000.7    unicast   MDFS RP:Statistics
    port_index = 0 seat_id = 0x10000 last sent = 0 last heard = 0
0/2/159
  10000.8    unicast   Slot 1 :MDFS.control.RIL
    port_index = 0 seat_id = 0x10000 last sent = 0 last heard = 0
0/0/0
RPC packets:current/peak/total
                                           0/1/4
```

This example shows how to display the contents of the IPC retransmission queue:

```
Switch> show ipc queue
There are 0 IPC messages waiting for acknowledgement in the transmit queue.
There are 0 IPC messages waiting for a response.
There are 0 IPC messages waiting for additional fragments.
There are 0 IPC messages currently on the IPC inboundQ.
Messages currently in use                :          3
Message cache size                       :         1000
Maximum message cache usage              :         1000

0 times message cache crossed            5000 [max]

Emergency messages currently in use      :          0

There are 2 messages currently reserved for reply msg.

Inbound message queue depth 0
Zone inbound message queue depth 0
```

This example shows how to display all the IPC session statistics:

```
Switch# show ipc session all
Tx Sessions:
Port ID      Type      Name
10000.7      Unicast   MDFS RP:Statistics
  port_index = 0  type = Unreliable  last sent = 0    last heard = 0
  Msgs requested = 180  Msgs returned = 180

10000.8      Unicast   Slot 1 :MDFS.control.RIL
  port_index = 0  type = Reliable    last sent = 0    last heard = 0
  Msgs requested = 0   Msgs returned = 0

Rx Sessions:
Port ID      Type      Name
10000.7      Unicast   MDFS RP:Statistics
  port_index = 0  seat_id = 0x10000  last sent = 0    last heard = 0
  No of msgs requested = 180  Msgs returned = 180

10000.8      Unicast   Slot 1 :MDFS.control.RIL
  port_index = 0  seat_id = 0x10000  last sent = 0    last heard = 0
  No of msgs requested = 0    Msgs returned = 0
```

This example shows how to display the status of the local IPC server:

```
Switch> show ipc status cumulative
IPC System Status

Time last IPC stat cleared :never

This processor is the IPC master server.
Do not drop output of IPC frames for test purposes.

1000 IPC Message Headers Cached.

                                     Rx Side    Tx Side
Total Frames                          12916      608
  0                                     0
Total from Local Ports                  13080      574
Total Protocol Control Frames           116        17
Total Frames Dropped                     0          0
```

## Service Usage

Total via Unreliable Connection-Less Service	12783	171
Total via Unreliable Sequenced Connection-Less Svc	0	0
Total via Reliable Connection-Oriented Service	17	116

<output truncated>

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">clear ipc</a>	Clears the IPC multicast routing statistics.

# show ipv6 access-list

Use the **show ipv6 access-list** user EXEC command to display the contents of all current IPv6 access lists.

```
show ipv6 access-list [access-list-name]
```



## Note

This command is available only if you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

## Syntax Description

*access-list-name* (Optional) Name of access list.

## Command Modes

User EXEC

## Command History

Release	Modification
12.2(50)SE	This command was introduced.

## Usage Guidelines

The **show ipv6 access-list** command provides output similar to the **show ip access-list** command, except that it is IPv6-specific.

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6 {default | routing | vlan}** global configuration command, and reload the switch.

## Examples

The following output from the **show ipv6 access-list** command shows IPv6 access lists named *inbound*:

```
Switch# show ipv6 access-list
IPv6 access list inbound
  permit tcp any any eq bgp (8 matches) sequence 10
  permit tcp any any eq telnet (15 matches) sequence 20
  permit udp any any sequence 30
```

**Table 2-15** show ipv6 access-list Field Descriptions

Field	Description
IPv6 access list inbound	Name of the IPv6 access list, for example, inbound.
permit	Permits any packet that matches the specified protocol type.
tcp	Transmission Control Protocol. The higher-level (Layer 4) protocol type that the packet must match.
any	Equal to ::/0.
eq	An equal operand that compares the source or destination ports of TCP or UDP packets.



**Table 2-15** show ipv6 access-list Field Descriptions (continued)

Field	Description
bgp (matches)	Border Gateway Protocol. The protocol type that the packet is equal to and the number of matches.
sequence 10	Sequence in which an incoming packet is compared to lines in an access list. Access list lines are ordered from first priority (lowest number, for example, 10) to last priority (highest number, for example, 80).

**Related Commands**

Command	Description
<b>clear ipv6 access-list</b>	Resets the IPv6 access list match counters.
<b>ipv6 access-list</b>	Defines an IPv6 access list and puts the switch into IPv6 access-list configuration mode.
<b>sdm prefer</b>	Configures an SDM template to optimize system resources based on how the switch is being used.

# show ipv6 dhcp conflict

Use the **show ipv6 dhcp conflict** privileged EXEC command to display address conflicts found by a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server when addresses are offered to the client.

**show ipv6 dhcp conflict**



## Note

This command is available only if the switch is running the metro IP access image and you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(50)SE	This command was introduced.

## Usage Guidelines

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6 {default | routing | vlan}** global configuration command, and reload the switch.

When you configure the DHCPv6 server to detect conflicts, it uses ping. The client uses neighbor discovery to detect clients and reports to the server through a DECLINE message. If an address conflict is detected, the address is removed from the pool, and the address cannot be assigned until it is removed from the conflict list.

## Examples

This is an example of the output from the **show ipv6 dhcp conflict** command:

```
Switch# show ipv6 dhcp conflict
Pool 350, prefix 2001:1005::/48
      2001:1005::10
```

## Related Commands

Command	Description
<a href="#">ipv6 dhcp pool</a>	Configures a DHCPv6 pool and enters DHCPv6 pool configuration mode.
<a href="#">clear ipv6 dhcp conflict</a>	Clears an address conflict from the DHCPv6 server database.

# show ipv6 route updated

Use the **show ipv6 route updated** user EXEC command to display the current contents of the IPv6 routing table.

```
show ipv6 route [protocol] updated [boot-up] {hh:mm | day{month [hh:mm]}} [{hh:mm | day{month [hh:mm]}}
```

Syntax Description		
<i>protocol</i>	(Optional) Display routes for the specified routing protocol. You can enter any of these keywords:	<ul style="list-style-type: none"> <li>• <b>eigrp</b></li> <li>• <b>ospf</b></li> <li>• <b>rip</b></li> </ul> or display routes for the specified type of route. You can enter any of these keywords: <ul style="list-style-type: none"> <li>• <b>connected</b></li> <li>• <b>local</b></li> <li>• <b>static</b></li> <li>• <b>interface</b> <i>interface id</i></li> </ul>
<b>boot-up</b>	Display the current contents of the IPv6 routing table.	
<i>hh:mm</i>	Enter the time as a 2-digit number for a 24-hour clock. Make sure to use the colons (:). For example, enter <b>13:32</b>	
<i>day</i>	Enter the day of the month. The range is from 1 to 31.	
<i>month</i>	Enter the month in upper case or lower case letters. You can enter the full name of the month, such as <b>January</b> or <b>august</b> , or the first three letters of the month, such as <b>jan</b> or <b>Aug</b> .	

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(50)SE	This command was introduced.

**Usage Guidelines** Use the **show ipv6 route** privileged EXEC command to display the current contents of the IPv6 routing table.

**Examples** This is an example of output from the **show ipv6 route updated rip** command.

```
Switch> show ipv6 route rip updated
IPv6 Routing Table - 12 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
```

## show ipv6 route updated

```

IA - ISIS interarea, IS - ISIS summary
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
R 2001::/64 [120/2]
via FE80::A8BB:CCFF:FE00:8D01, GigabitEthernet0/1
Last updated 10:31:10 27 February 2007
R 2004::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet0/2
Last updated 17:23:05 22 February 2007
R 4000::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet0/3
Last updated 17:23:05 22 February 2007
R 5000::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet0/4
Last updated 17:23:05 22 February 2007
R 5001::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet0/5
Last updated 17:23:05 22 February 2008

```

### Related Commands

Command	Description
<b>show ipv6 route</b>	Displays the current contents of the IPv6 routing table. For syntax information, select <b>Cisco IOS Software &gt; Command References for the Cisco IOS Software Releases 12.3 Mainline &gt; Cisco IOS IPv6 Command Reference &gt; IPv6 Commands: show ipv6 nat translations through show ipv6 protocols</b>

# show l2protocol-tunnel

Use the **show l2protocol-tunnel** user EXEC command to display information about Layer 2 protocol tunnel ports. Displays information for interfaces with protocol tunneling enabled.

**show l2protocol-tunnel** [**interface** *interface-id*] [**summary**]

<b>Syntax Description</b>	<b>interface</b> <i>interface-id</i> (Optional) Specify the interface for which protocol tunneling information appears. Valid interfaces are physical ports and port channels; the port channel range is 1 to 64.
	<b>summary</b> (Optional) Display only Layer 2 protocol summary information.

<b>Command Modes</b>	User EXEC
----------------------	-----------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

**Usage Guidelines** After enabling Layer 2 protocol tunneling on an access port, a trunk port, or an IEEE 802.1Q tunnel port by using the **l2protocol-tunnel** interface configuration command, you can configure some or all of these parameters:

- Protocol type to be tunneled
- Shutdown threshold
- Drop threshold

If you enter the **show l2protocol-tunnel** [**interface** *interface-id*] command, only information about the active ports on which all the parameters are configured appears.

If you enter the **show l2protocol-tunnel summary** command, only information about the active ports on which some or all of the parameters are configured appears.

## show l2protocol-tunnel

### Examples

This is an example of output from the **show l2protocol-tunnel** command:

```
Switch> show l2protocol-tunnel
COS for Encapsulated Packets: 5
Drop Threshold for Encapsulated Packets: 0
```

Port	Protocol	Shutdown Threshold	Drop Threshold	Encapsulation Counter	Decapsulation Counter	Drop Counter
Fa0/3	---	----	----	----	----	----
	---	----	----	----	----	----
	---	----	----	----	----	----
	pagp	----	----	0	242500	
	lacp	----	----	24268	242640	
Fa0/4	udld	----	----	0	897960	
	---	----	----	----	----	----
	---	----	----	----	----	----
	pagp	1000	----	24249	242700	
	lacp	----	----	24256	242660	
Gi0/1	udld	----	----	0	897960	
	cdp	----	----	134482	1344820	
	---	----	----	----	----	----
	---	----	----	----	----	----
	pagp	1000	----	0	242500	
	lacp	500	----	0	485320	
	udld	300	----	44899	448980	

This is an example of output from the **show l2protocol-tunnel summary** command:

```
Switch> show l2protocol-tunnel summary
COS for Encapsulated Packets: 5
Drop Threshold for Encapsulated Packets: 0
```

Port	Protocol	Shutdown Threshold (cdp/stp/vtp) (pagp/lacp/udld)	Drop Threshold (cdp/stp/vtp) (pagp/lacp/udld)	Status
Fa0/2	---	----/----/----	----/----/----	up
	pagp lacp udld	----/----/----	----/----/----	
Fa0/3	---	----/----/----	----/----/----	up
	pagp lacp udld	1000/----/----	----/----/----	
Fa0/4	---	----/----/----	----/----/----	up
	pagp lacp udld	1000/ 500/----	----/----/----	
Fa0/5	cdp stp vtp	----/----/----	----/----/----	down
	---	----/----/----	----/----/----	
Gi0/1	---	----/----/----	----/----/----	down
	pagp	----/----/----	1000/----/----	
Gi0/2	---	----/----/----	----/----/----	down
	pagp	----/----/----	1000/----/----	

### Related Commands

Command	Description
<a href="#">clear l2protocol-tunnel counters</a>	Clears counters for protocol tunneling ports.
<a href="#">l2protocol-tunnel</a>	Enables Layer 2 protocol tunneling for CDP, STP, or VTP packets on an interface.
<a href="#">l2protocol-tunnel cos</a>	Configures a class of service (CoS) value for tunneled Layer 2 protocol packets.

# show lacp

Use the **show lacp** user EXEC command to display Link Aggregation Control Protocol (LACP) channel-group information.

```
show lacp [channel-group-number] { counters | internal | neighbor | sys-id }
```



## Note

LACP is available only on network node interfaces (NNIs) or enhanced network interfaces (ENIs).

## Syntax Description

<i>channel-group-number</i>	(Optional) Number of the channel group. The range is 1 to 48.
<b>counters</b>	Display traffic information.
<b>internal</b>	Display internal information.
<b>neighbor</b>	Display neighbor information.
<b>sys-id</b>	Display the system identifier that is being used by LACP. The system identifier is made up of the LACP system priority and the switch MAC address.

## Command Modes

User EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

You can enter any **show lacp** command to display the active channel-group information. To display specific channel information, enter the **show lacp** command with a channel-group number.

If you do not specify a channel group, information for all channel groups appears.

You can enter the *channel-group-number* option to specify a channel group for all keywords except **sys-id**.

## ■ show lacp

**Examples**

This is an example of output from the **show lacp counters** user EXEC command. [Table 2-16](#) describes the fields in the display.

```
Switch> show lacp counters
          LACPDU      Marker      Marker Response      LACPDU
Port      Sent   Recv   Sent   Recv   Sent   Recv   Pkts Err
-----
Channel group:1
Gi0/1      19    10     0     0     0     0     0
Gi0/2      14     6     0     0     0     0     0
```

**Table 2-16** *show lacp counters Field Descriptions*

Field	Description
LACPDU Sent and Recv	The number of LACP packets sent and received by a port.
Marker Sent and Recv	The number of LACP marker packets sent and received by a port.
Marker Response Sent and Recv	The number of LACP marker response packets sent and received by a port.
LACPDU Pkts and Err	The number of unknown and illegal packets received by LACP for a port.

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

```
Switch> show lacp 1 internal
Flags:  S - Device is requesting Slow LACPDU
        F - Device is requesting Fast LACPDU
        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      State  Priority  Key         Key     Key   Number State
Gi0/1    SA     bndl     32768      0x3     0x3   0x4   0x3D
Gi0/2    SA     bndl     32768      0x3     0x3   0x5   0x3D
```

[Table 2-17](#) describes the fields in the display.

**Table 2-17** *show lacp internal Field Descriptions*

Field	Description
State	State of the specific port. These are the allowed values: <ul style="list-style-type: none"> <li>—Port is in an unknown state.</li> <li><b>bndl</b>—Port is attached to an aggregator and bundled with other ports.</li> <li><b>susp</b>—Port is in a suspended state; it is not attached to any aggregator.</li> <li><b>hot-sby</b>—Port is in a hot-standby state.</li> <li><b>indiv</b>—Port is incapable of bundling with any other port.</li> <li><b>indep</b>—Port is in an independent state (not bundled but able to switch data traffic. In this case, LACP is not running on the partner port).</li> <li><b>down</b>—Port is down.</li> </ul>
LACP Port Priority	Port priority setting. LACP uses the port priority to put ports s in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.



Table 2-17 show lacp internal Field Descriptions (continued)

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"> <li>• bit0: LACP_Activity</li> <li>• bit1: LACP_Timeout</li> <li>• bit2: Aggregation</li> <li>• bit3: Synchronization</li> <li>• bit4: Collecting</li> <li>• bit5: Distributing</li> <li>• bit6: Defaulted</li> <li>• bit7: Expired</li> </ul> <p><b>Note</b> In the above list, bit7 is the MSB and bit0 is the LSB.</p>

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

```
Switch> show lacp neighbor
Flags: S - Device is sending Slow LACPDUs F - Device is sending Fast LACPDUs
       A - Device is in Active mode       P - Device is in Passive mode

Channel group 3 neighbors

Partner's information:

Port      Partner          Partner          Partner
System ID System ID        Port Number      Age             Flags
Gi0/1    32768,0007.eb49.5e80 0xC              19s            SP

          LACP Partner    Partner          Partner
          Port Priority   Oper Key         Port State
          32768             0x3              0x3C

Partner's information:

Port      Partner          Partner          Partner
System ID System ID        Port Number      Age             Flags
Gi0/2    32768,0007.eb49.5e80 0xD              15s            SP

          LACP Partner    Partner          Partner
          Port Priority   Oper Key         Port State
          32768             0x3              0x3C
```

**show lacp**

This is an example of output from the **show lacp sys-id** command:

```
Switch> show lacp sys-id  
32765,0002.4b29.3a00
```

The system identification is made up of the system priority and the system MAC address. The first two bytes are the system priority, and the last six bytes are the globally administered individual MAC address associated to the system.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">clear lacp</a>	Clears the LACP channel-group information.
<a href="#">lacp port-priority</a>	Configures the LACP port priority.
<a href="#">lacp system-priority</a>	Configures the LACP system priority.

# show link state group

Use the **show link state group** global configuration command to display the link-state group information.

**show link state group** [*number*] [**detail**]

Syntax Description	
<i>number</i>	(Optional) Number of the link-state group.
<b>detail</b>	(Optional) Specify that detailed information appears.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** Use the **show link state group** command to display the link-state group information. Enter this command without keywords to display information about all link-state groups. Enter the group number to display information specific to the group.

Enter the **detail** keyword to display detailed information about the group. The output for the **show link state group detail** command displays only those link-state groups that have link-state tracking enabled or that have upstream or downstream interfaces (or both) configured. If there is no link-state group configuration for a group, it is not shown as enabled or disabled.

**Examples** This is an example of output from the **show link state group 1** command:

```
Switch> show link state group 1
Link State Group: 1      Status: Enabled, Down
```

## show link state group

This is an example of output from the **show link state group detail** command:

```
Switch> show link state group detail
(Up):Interface up   (Dwn):Interface Down   (Dis):Interface disabled

Link State Group: 1 Status: Enabled, Down
Upstream Interfaces : Gi0/15(Dwn) Gi0/16(Dwn)
Downstream Interfaces : Gi0/11(Dis) Gi0/12(Dis) Gi0/13(Dis) Gi0/14(Dis)

Link State Group: 2 Status: Enabled, Down
Upstream Interfaces : Gi0/15(Dwn) Gi0/16(Dwn) Gi0/17(Dwn)
Downstream Interfaces : Gi0/11(Dis) Gi0/12(Dis) Gi0/13(Dis) Gi0/14(Dis)

(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
```

### Related Commands

Command	Description
<a href="#">link state group</a>	Configures an interface as a member of a link-state group.
<a href="#">link state track</a>	Enables a link-state group.
<a href="#">show running-config</a>	Displays the operating configuration.

# show location

Use the **show location** user EXEC command to display location information for an endpoint.

**show location admin-tag**

**show location civic-location** { **identifier** *id number* | **interface** *interface-id* | **static** }

**show location elin-location** { **identifier** *id number* | **interface** *interface-id* | **static** }

Syntax Description		
<b>admin-tag</b>		Display administrative tag or site information.
<b>civic-location</b>		Display civic location information.
<b>elin-location</b>		Display emergency location information (ELIN).
<b>identifier</b> <i>id</i>		Specify the ID for the civic location or the elin location. The id range is 1 to 4095.
<b>interface</b> <i>interface-id</i>		Display location information for the specified interface or all interfaces. Valid interfaces include physical ports.
<b>static</b>		Display static configuration information.

**Command Modes** User EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** Use the **show location** command to display location information for an endpoint.

**Examples**

This is an example of output from the **show location civic-location** command that displays location information for an interface:

```
Switch> show location civic interface gigabitethernet2/0/1
Civic location information
-----
Identifier          : 1
County              : Santa Clara
Street number       : 3550
Building            : 19
Room                : C6
Primary road name   : Cisco Way
City                : San Jose
State               : CA
Country             : US
```

This is an example of output from the **show location civic-location** command that displays all the civic location information:

```
Switch> show location civic-location static
Civic location information
-----
Identifier          : 1
County              : Santa Clara
Street number       : 3550
Building            : 19
Room                : C6
Primary road name   : Cisco Way
City                : San Jose
State               : CA
Country             : US
Ports               : Gi2/0/1
-----
Identifier          : 2
Street number       : 24568
Street number suffix : West
Landmark            : Golden Gate Bridge
Primary road name   : 19th Ave
City                : San Francisco
Country             : US
-----
```

This is an example of output from the **show location elin-location** command that displays the emergency location information:

```
Switch> show location elin-location identifier 1
Elin location information
-----
Identifier : 1
Elin      : 14085553881
Ports     : Gi2/0/2
```

This is an example of output from the **show location elin static** command that displays all emergency location information:

```
Switch> show location elin static
Elin location information
-----
Identifier : 1
Elin      : 14085553881
Ports    : Gi2/0/2
-----
Identifier : 2
Elin      : 18002228999
-----
```

#### Related Commands

Command	Description
<a href="#">location (global configuration)</a>	Configures the global location information for an endpoint.
<a href="#">location (interface configuration)</a>	Configures the location information for an interface.

# show logging onboard

Use the **show logging onboard** privileged EXEC command to display the on-board failure logging (OBFL) information.

```
show logging onboard [module slot-number] { { clilog | environment | message | temperature |
uptime | voltage } [ continuous | detail | summary ] [ start hh:mm:ss day month year ] [ end
hh:mm:ss day month year ] }
```

Syntax Description		
<b>module</b> <i>slot-number</i>	(Optional) The <b>module</b> slot number is always 1 and is not relevant for the ME-3400E.	
<b>clilog</b>	Display the OBFL CLI commands that were entered on the switch.	
<b>environment</b>	Display the unique device identifier (UDI) information for the switch and for all the connected devices: the product identification (PID), the version identification (VID), and the serial number.	
<b>message</b>	Display the hardware-related system messages generated by the switch.	
<b>temperature</b>	Display the temperature of the switch.	
<b>uptime</b>	Display the time when the switch starts, the reason the switch restarts, and the length of time the switch has been running since it last restarted.	
<b>voltage</b>	Display the system voltages of the switch.	
<b>continuous</b>	(Optional) Display the data in the <i>continuous</i> file. For more information, see the “Usage Guidelines” section.	
<b>summary</b>	(Optional) Display the data in the <i>summary</i> file. For more information, see the “Usage Guidelines” section.	
<b>start</b> <i>hh:mm:ss day month year</i>	(Optional) Display the data from the specified time and date. For more information, see the “Usage Guidelines” section.	
<b>end</b> <i>hh:mm:ss day month year</i>	(Optional) Display the data up to the specified time and date. For more information, see the “Usage Guidelines” section.	
<b>detail</b>	(Optional) Display both the continuous and summary data.	

**Defaults** There is no default.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** When OBFL is enabled, the switch records all the OBFL data in a continuous, circular file. When the continuous file is full, the switch combines the data into a summary file, which is also known as a historical file. The switch then continues to write new data to the continuous file.



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 2-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 upper-case or lower-case 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.

## Examples

This is an example of 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 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 is an example of output from the **show logging onboard message** command:

```
Switch# show logging onboard message
-----
ERROR MESSAGE SUMMARY INFORMATION
-----
Facility-Sev-Name      | Count | Persistence Flag
MM/DD/YYYY HH:MM:SS
-----
No historical data to display
-----
```

This is an example of 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 cliilog :
      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 is an example of 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 is an example of 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 is an example of 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
-----
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
-----
```

### Related Commands

Command	Description
<a href="#">clear logging onboard</a>	Removes the OBFL data in the flash memory.
<a href="#">hw-module module logging onboard</a>	Enables OBFL.

## show mac access-group

Use the **show mac access-group** user EXEC command to display the MAC access control lists (ACLs) configured for an interface or a switch.

```
show mac access-group [interface interface-id]
```

<b>Syntax Description</b>	<b>interface</b> <i>interface-id</i> (Optional) Display the MAC ACLs configured on a specific interface. Valid interfaces are physical ports and port channels; the port-channel range is 1 to 48 (available only in privileged EXEC mode).
---------------------------	---

<b>Command Modes</b>	User EXEC
----------------------	-----------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

**Examples** This is an example of output from the **show mac-access group** user EXEC command. In this display, Fast Ethernet interface 0/2 has the MAC access list *macl\_e1* applied to inbound traffic; no MAC ACLs are applied to other interfaces.

```
Switch> show mac access-group
Interface FastEthernet0/1:
  Inbound access-list is macl_e1
  Outbound access-list is not set
Interface FastEthernet0/2:
  Inbound access-list is not set
  Outbound access-list is not set
Interface FastEthernet0/3:
  Inbound access-list is not set
  Outbound access-list is not set
Interface FastEthernet0/4:
  Inbound access-list is not set
  Outbound access-list is not set
Interface FastEthernetv0/5:
  Inbound access-list is not set
  Outbound access-list is not set
<output truncated>
```

This is an example of output from the **show mac access-group interface fastethernet0/1** command:

```
Switch# show mac access-group interface fastethernet0/1
Interface FastEthernet0/1:
  Inbound access-list is macl_e1
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">mac access-group</a>	Applies a MAC access group to an interface.

# show mac address-table

Use the **show mac address-table** user EXEC command to display a specific MAC address table static and dynamic entry or the MAC address table static and dynamic entries on a specific interface or VLAN.

## show mac address-table

**Syntax Description** This command has no arguments or keywords.

**Command Modes** User EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Examples** This is an example of output from the **show mac address-table** command:

```
Switch> show mac address-table
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
-----
  All    0000.0000.0001   STATIC  CPU
  All    0000.0000.0002   STATIC  CPU
  All    0000.0000.0003   STATIC  CPU
  All    0000.0000.0009   STATIC  CPU
  All    0000.0000.0012   STATIC  CPU
  All    0180.c200.000b   STATIC  CPU
  All    0180.c200.000c   STATIC  CPU
  All    0180.c200.000d   STATIC  CPU
  All    0180.c200.000e   STATIC  CPU
  All    0180.c200.000f   STATIC  CPU
  All    0180.c200.0010   STATIC  CPU
  1      0030.9441.6327   DYNAMIC Gi0/4
Total Mac Addresses for this criterion: 12
```

Related Commands	Command	Description
	<b>clear mac address-table dynamic</b>	Deletes from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, or all dynamic addresses on a particular VLAN.
	<b>show mac address-table aging-time</b>	Displays the aging time in all VLANs or the specified VLAN.
	<b>show mac address-table count</b>	Displays the number of addresses present in all VLANs or the specified VLAN.
	<b>show mac address-table dynamic</b>	Displays dynamic MAC address table entries only.
	<b>show mac address-table interface</b>	Displays the MAC address table information for the specified interface.
	<b>show mac address-table notification</b>	Displays the MAC address notification settings for all interfaces or the specified interface.
	<b>show mac address-table static</b>	Displays static MAC address table entries only.
	<b>show mac address-table vlan</b>	Displays the MAC address table information for the specified VLAN.

# show mac address-table address

Use the **show mac address-table address** user EXEC command to display MAC address table information for the specified MAC address.

**show mac address-table address** *mac-address* [**interface** *interface-id*] [**vlan** *vlan-id*]

Syntax Description	
<i>mac-address</i>	Specify the 48-bit MAC address; the valid format is H.H.H.
<b>interface</b> <i>interface-id</i>	(Optional) Display information for a specific interface. Valid interfaces include physical ports and port channels.
<b>vlan</b> <i>vlan-id</i>	(Optional) Display entries for the specific VLAN only. The range is 1 to 4094.

**Command Modes** User EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

## Examples

This is an example of output from the **show mac address-table address** command:

```
Switch# show mac address-table address 0002.4b28.c482
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
All     0002.4b28.c482  STATIC  CPU
Total Mac Addresses for this criterion: 1
```

Related Commands	Command	Description
	<a href="#">show mac address-table aging-time</a>	Displays the aging time in all VLANs or the specified VLAN.
	<a href="#">show mac address-table count</a>	Displays the number of addresses present in all VLANs or the specified VLAN.
	<a href="#">show mac address-table dynamic</a>	Displays dynamic MAC address table entries only.
	<a href="#">show mac address-table interface</a>	Displays the MAC address table information for the specified interface.
	<a href="#">show mac address-table notification</a>	Displays the MAC address notification settings for all interfaces or the specified interface.
	<a href="#">show mac address-table static</a>	Displays static MAC address table entries only.
	<a href="#">show mac address-table vlan</a>	Displays the MAC address table information for the specified VLAN.

## show mac address-table aging-time

Use the **show mac address-table aging-time** user EXEC command to display the aging time of a specific address table instance, all address table instances on a specified VLAN or, if a specific VLAN is not specified, on all VLANs.

**show mac address-table aging-time** [**vlan** *vlan-id*]

<b>Syntax Description</b>	<b>vlan</b> <i>vlan-id</i>	(Optional) Display aging time information for a specific VLAN. The range is 1 to 4094.
---------------------------	----------------------------	--

<b>Command Modes</b>	User EXEC
----------------------	-----------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

<b>Usage Guidelines</b>	If no VLAN number is specified, the aging time for all VLANs appears.
-------------------------	---

**Examples** This is an example of output from the **show mac address-table aging-time** command:

```
Switch> show mac address-table aging-time
Vlan    Aging Time
----    -
  1      300
```

This is an example of output from the **show mac address-table aging-time vlan 10** command:

```
Switch> show mac address-table aging-time vlan 10
Vlan    Aging Time
----    -
  10     300
```



Related Commands	Command	Description
	<a href="#">mac address-table aging-time</a>	Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated.
	<a href="#">show mac address-table address</a>	Displays MAC address table information for the specified MAC address.
	<a href="#">show mac address-table count</a>	Displays the number of addresses present in all VLANs or the specified VLAN.
	<a href="#">show mac address-table dynamic</a>	Displays dynamic MAC address table entries only.
	<a href="#">show mac address-table interface</a>	Displays the MAC address table information for the specified interface.
	<a href="#">show mac address-table notification</a>	Displays the MAC address notification settings for all interfaces or the specified interface.
	<a href="#">show mac address-table static</a>	Displays static MAC address table entries only.
	<a href="#">show mac address-table vlan</a>	Displays the MAC address table information for the specified VLAN.

# show mac address-table count

Use the **show mac address-table count** user EXEC command to display the number of addresses present in all VLANs or the specified VLAN.

**show mac address-table count** [**vlan** *vlan-id*]

<b>Syntax Description</b>	<b>vlan</b> <i>vlan-id</i> (Optional) Display the number of addresses for a specific VLAN. The range is 1 to 4094.
---------------------------	--

<b>Command Modes</b>	User EXEC
----------------------	-----------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

<b>Usage Guidelines</b>	If no VLAN number is specified, the address count for all VLANs appears.
-------------------------	--

<b>Examples</b>	This is an example of output from the <b>show mac address-table count</b> command:
-----------------	--

```
Switch# show mac address-table count
Mac Entries for Vlan : 1
-----
Dynamic Address Count : 2
Static Address Count : 0
Total Mac Addresses : 2
```

Related Commands	Command	Description
	<code>show mac address-table address</code>	Displays MAC address table information for the specified MAC address.
	<code>show mac address-table aging-time</code>	Displays the aging time in all VLANs or the specified VLAN.
	<code>show mac address-table dynamic</code>	Displays dynamic MAC address table entries only.
	<code>show mac address-table interface</code>	Displays the MAC address table information for the specified interface.
	<code>show mac address-table notification</code>	Displays the MAC address notification settings for all interfaces or the specified interface.
	<code>show mac address-table static</code>	Displays static MAC address table entries only.
	<code>show mac address-table vlan</code>	Displays the MAC address table information for the specified VLAN.

## show mac address-table dynamic

Use the **show mac address-table dynamic** user EXEC command to display only dynamic MAC address table entries.

```
show mac address-table dynamic [address mac-address] [interface interface-id] [vlan vlan-id]
```

### Syntax Description

<b>address</b> <i>mac-address</i>	(Optional) Specify a 48-bit MAC address; the valid format is H.H.H (available in privileged EXEC mode only).
<b>interface</b> <i>interface-id</i>	(Optional) Specify an interface to match; valid <i>interfaces</i> include physical ports and port channels.
<b>vlan</b> <i>vlan-id</i>	(Optional) Display entries for a specific VLAN; the range is 1 to 4094.

### Command Modes

User EXEC

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Examples

This is an example of output from the **show mac address-table dynamic** command:

```
Switch> show mac address-table dynamic
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
1       0030.b635.7862   DYNAMIC Gi0/2
1       00b0.6496.2741   DYNAMIC Gi0/2
Total Mac Addresses for this criterion: 2
```

Related Commands	Command	Description
	<b>clear mac address-table dynamic</b>	Deletes from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, or all dynamic addresses on a particular VLAN.
	<b>show mac address-table address</b>	Displays MAC address table information for the specified MAC address.
	<b>show mac address-table aging-time</b>	Displays the aging time in all VLANs or the specified VLAN.
	<b>show mac address-table count</b>	Displays the number of addresses present in all VLANs or the specified VLAN.
	<b>show mac address-table interface</b>	Displays the MAC address table information for the specified interface.
	<b>show mac address-table static</b>	Displays static MAC address table entries only.
	<b>show mac address-table vlan</b>	Displays the MAC address table information for the specified VLAN.

## show mac address-table interface

Use the **show mac address-table interface** user command to display the MAC address table information for the specified interface in the specified VLAN.

```
show mac address-table interface interface-id [vlan vlan-id]
```

### Syntax Description

<i>interface-id</i>	Specify an interface type; valid interfaces include physical ports and port channels.
<b>vlan</b> <i>vlan-id</i>	(Optional) Display entries for a specific VLAN; the range is 1 to 4094.

### Command Modes

User EXEC

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Examples

This is an example of output from the **show mac address-table interface** command:

```
Switch> show mac address-table interface gigabitethernet0/2
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
1       0030.b635.7862   DYNAMIC Gi0/2
1       00b0.6496.2741   DYNAMIC Gi0/2
Total Mac Addresses for this criterion: 2
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show mac address-table address</b>	Displays MAC address table information for the specified MAC address.
<b>show mac address-table aging-time</b>	Displays the aging time in all VLANs or the specified VLAN.
<b>show mac address-table count</b>	Displays the number of addresses present in all VLANs or the specified VLAN.
<b>show mac address-table dynamic</b>	Displays dynamic MAC address table entries only.
<b>show mac address-table notification</b>	Displays the MAC address notification settings for all interfaces or the specified interface.
<b>show mac address-table static</b>	Displays static MAC address table entries only.
<b>show mac address-table vlan</b>	Displays the MAC address table information for the specified VLAN.

## show mac address-table learning

Use the **show mac address-table learning** user EXEC command to display the status of MAC address learning for all VLANs or the specified VLAN.

**show mac address-table learning** [**vlan** *vlan-id*]

<b>Syntax Description</b>	<b>vlan</b> <i>vlan-id</i>	(Optional) Display information for a specific VLAN. The range is 1 to 4094.
---------------------------	----------------------------	---

<b>Command Modes</b>	User EXEC
----------------------	-----------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

<b>Usage Guidelines</b>	Use the <b>show mac address-table learning</b> 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.
-------------------------	--

<b>Examples</b>	This is an example of output from the <b>show mac address-table learning</b> user EXEC 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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">mac address-table learning vlan</a>	Enables or disables MAC address learning on a VLAN.



# show mac address-table move update

Use the **show mac address-table move update** user EXEC command to display the MAC address-table move update information on the switch.

## show mac address-table move update

**Syntax Description** This command has no arguments or keywords.

**Command Modes** User EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Examples** This is an example of output from the **show mac address-table move update** command:

```
Switch> 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
switch#
```

Related Commands	Command	Description
	<a href="#">clear mac address-table move update</a>	Clears the MAC address-table move update counters.
	<a href="#">mac address-table move update {receive   transmit}</a>	Configures MAC address-table move update on the switch.

# show mac address-table notification

Use the **show mac address-table notification** user EXEC command to display the MAC address notification settings for all interfaces or the specified interface.

**show mac address-table notification { change [interface *interface-id*] | mac-move | threshold }**

## Syntax Description

<b>change</b>	Display the MAC change notification feature parameters and the history table.
<b>interface</b>	(Optional) Display information for all interfaces. Valid interfaces include physical ports and port channels.
<i>interface-id</i>	(Optional) Display information for the specified interface. Valid interfaces include physical ports and port channels.
<b>mac-move</b>	Display status for MAC address move notifications.
<b>threshold</b>	Display status for MAC-address table threshold monitoring.

## Command Modes

User EXEC

## Command History

Release	Modification
12.2(44)EY	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 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.

## Examples

This is an example of 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: 0000.0000.0000 Module: 0   Port: 1
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

```

### Related Commands

Command	Description
<b>clear mac address-table notification</b>	Clears the MAC address notification global counters.
<b>show mac address-table address</b>	Displays MAC address table information for the specified MAC address.
<b>show mac address-table aging-time</b>	Displays the aging time in all VLANs or the specified VLAN.
<b>show mac address-table count</b>	Displays the number of addresses present in all VLANs or the specified VLAN.
<b>show mac address-table dynamic</b>	Displays dynamic MAC address table entries only.
<b>show mac address-table interface</b>	Displays the MAC address table information for the specified interface.
<b>show mac address-table static</b>	Displays static MAC address table entries only.
<b>show mac address-table vlan</b>	Displays the MAC address table information for the specified VLAN.

# show mac address-table static

Use the **show mac address-table static** user EXEC command to display only static MAC address table entries.

```
show mac address-table static [address mac-address] [interface interface-id] [vlan vlan-id]
```

## Syntax Description

<b>address mac-address</b>	(Optional) Specify a 48-bit MAC address; the valid format is H.H.H (available in privileged EXEC mode only).
<b>interface interface-id</b>	(Optional) Specify an interface to match; valid <i>interfaces</i> include physical ports and port channels.
<b>vlan vlan-id</b>	(Optional) Display addresses for a specific VLAN. The range is 1 to 4094.

## Command Modes

User EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Examples

This is an example of output from the **show mac address-table static** command:

```
Switch> show mac address-table static

      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
All     0100.0ccc.cccc  STATIC  CPU
All     0180.c200.0000  STATIC  CPU
All     0100.0ccc.cccd  STATIC  CPU
All     0180.c200.0001  STATIC  CPU
All     0180.c200.0004  STATIC  CPU
All     0180.c200.0005  STATIC  CPU
  4     0001.0002.0004  STATIC  Drop
  6     0001.0002.0007  STATIC  Drop
Total Mac Addresses for this criterion: 8
```

## Related Commands

Command	Description
<a href="#">mac address-table static</a>	Adds static addresses to the MAC address table.
<a href="#">mac address-table static drop</a>	Enables unicast MAC address filtering and configures the switch to drop traffic with a specific source or destination MAC address.
<a href="#">show mac address-table address</a>	Displays MAC address table information for the specified MAC address.
<a href="#">show mac address-table aging-time</a>	Displays the aging time in all VLANs or the specified VLAN.

Command	Description
<b>show mac address-table count</b>	Displays the number of addresses present in all VLANs or the specified VLAN.
<b>show mac address-table dynamic</b>	Displays dynamic MAC address table entries only.
<b>show mac address-table interface</b>	Displays the MAC address table information for the specified interface.
<b>show mac address-table notification</b>	Displays the MAC address notification settings for all interfaces or the specified interface.
<b>show mac address-table vlan</b>	Displays the MAC address table information for the specified VLAN.

## show mac address-table vlan

Use the **show mac address-table vlan** user EXEC command to display the MAC address table information for the specified VLAN.

**show mac address-table vlan** *vlan-id*

Syntax Description	<i>vlan-id</i> (Optional) Display addresses for a specific VLAN. The range is 1 to 4094.
--------------------	--

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

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

### Examples

This is an example of output from the **show mac address-table vlan 1** command:

```
Switch> show mac address-table vlan 1
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
  1     0100.0ccc.cccc  STATIC CPU
  1     0180.c200.0000  STATIC CPU
  1     0100.0ccc.cccd  STATIC CPU
  1     0180.c200.0001  STATIC CPU
  1     0180.c200.0002  STATIC CPU
  1     0180.c200.0003  STATIC CPU
  1     0180.c200.0005  STATIC CPU
  1     0180.c200.0006  STATIC CPU
  1     0180.c200.0007  STATIC CPU
Total Mac Addresses for this criterion: 9
```

Related Commands	Command	Description
	<b>show mac address-table address</b>	Displays MAC address table information for the specified MAC address.
	<b>show mac address-table aging-time</b>	Displays the aging time in all VLANs or the specified VLAN.
	<b>show mac address-table count</b>	Displays the number of addresses present in all VLANs or the specified VLAN.
	<b>show mac address-table dynamic</b>	Displays dynamic MAC address table entries only.
	<b>show mac address-table interface</b>	Displays the MAC address table information for the specified interface.
	<b>show mac address-table notification</b>	Displays the MAC address notification settings for all interfaces or the specified interface.
	<b>show mac address-table static</b>	Displays static MAC address table entries only.

# show monitor

Use the **show monitor** user EXEC command to display information about all Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) sessions on the switch. Use the command with keywords to show a specific session, all sessions, all local sessions, or all remote sessions.

**show monitor** [**session** {*session\_number* | **all** | **local** | **range** *list* | **remote**} [**detail**]]

## Syntax Description

<b>session</b>	(Optional) Display information about specified SPAN sessions.
<i>session_number</i>	Specify the number of the SPAN or RSPAN session. The range is 1 to 66.
<b>all</b>	Display all SPAN sessions.
<b>local</b>	Display only local SPAN sessions.
<b>range</b> <i>list</i>	Display a range of SPAN sessions, where <i>list</i> is the range of valid sessions, either a single session or a range of sessions described by two numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated parameters or in hyphen-specified ranges.  <b>Note</b> This keyword is available only in privileged EXEC mode.
<b>remote</b>	Display only remote SPAN sessions.
<b>detail</b>	(Optional) Display detailed information about the specified sessions.

## Command Modes

User EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The output is the same for the **show monitor** command and the **show monitor session all** command.



**Examples**

This is an example of output for the **show monitor** user EXEC command:

```
Switch# show monitor
Session 1
-----
Type           :Local Session
Source Ports:
  RX Only:      Fa0/24
  TX Only:      None
  Both:         Fa0/1-2,Fa0/1-5
Destination Ports:Fa0/18
Encapsulation:Replicate

Session 2
-----
Type           :Remote Source Session
Source Ports:
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 RSPAN source session 1:

```
Switch# show monitor session 1
Session 1
-----
Type           :Local Session
Source Ports:
  RX Only:      Fa0/24
  TX Only:      None
  Both:         Fa0/1-2,Fa0/1-5
Destination Ports:Fa0/18
Encapsulation:Replicate
```

This is an example of output for the **show monitor session all** user EXEC command when ingress traffic forwarding is enabled:

```
Switch# show monitor session all
Session 1
-----
Type           :Local Session
Source Ports   :
  Both         :Fa0/2
Destination Ports :Fa0/3
Encapsulation  :Replicate
  Ingress:Enabled, default VLAN = 5
  Ingress encapsulation:DOT1Q

Session 2
-----
Type           :Local Session
Source Ports   :
  Both         :Fa0/1
Destination Ports :Fa0/4
Encapsulation  :Replicate
  Ingress:Enabled
  Ingress encapsulation:DOT1Q
```

**Related Commands**

Command	Description
<a href="#">monitor session</a>	Starts or modifies a SPAN or RSPAN session.

## show mvr

Use the **show mvr** privileged EXEC command without keywords 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).

**show mvr**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Modes** Privileged EXEC

---

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

---



---

**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).

Related Commands	Command	Description
	<a href="#">mvr (global configuration)</a>	Enables and configures multicast VLAN registration on the switch.
	<a href="#">mvr (interface configuration)</a>	Configures MVR ports.
	<a href="#">show mvr interface</a>	Displays the configured MVR interfaces, status of the specified interface, or all multicast groups to which the interface belongs when the <b>interface</b> and <b>members</b> keywords are appended to the command.
	<a href="#">show mvr members</a>	Displays all ports that are members of an MVR multicast group or, if there are no members, means the group is inactive.

## show mvr interface

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

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

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

Command Modes	
	Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

Usage Guidelines	
	<p>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.</p> <p>If you enter the <b>show mvr interface</b> <i>interface-id</i> command and the specified port is a non-MVR port, the output displays NON MVR in the Type field. For active MVR ports, it displays the port type (RECEIVER or SOURCE), mode (access or trunk), VLAN, status, and Immediate-Leave setting.</p> <p>If you enter the <b>members</b> keyword, all MVR group members on the interface appear.</p>

**Examples**

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

```
Switch# show mvr interface
Port      Type           Mode           VLAN    Status           Immediate Leave
-----
Fa0/1     Receiver       Trunk          1       ACTIVE/UP        DISABLED
Fa0/1     Receiver       Trunk          2000    ACTIVE/DOWN      DISABLED
Fa0/2     Receiver       Trunk          2       ACTIVE/UP        DISABLED
Fa0/2     Receiver       Trunk          3000    ACTIVE/UP        DISABLED
Fa0/3     Receiver       Trunk          2       ACTIVE/UP        DISABLED
Fa0/3     Receiver       Trunk          3000    ACTIVE/UP        DISABLED
Fa0/10    Source         Access         10      ACTIVE/UP        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 fastethernet0/10** command:

```
switch# show mvr interface fa0/10
Port      Type           Mode           VLAN    Status           Immediate Leave
-----
Fa0/10    RECEIVER       Trunk          201     ACTIVE/DOWN      DISABLED
```

This is an example of output from the **show mvr interface fastethernet0/1** command. In this example, the port is not an MVR member:

```
switch# show mvr interface fa0/1
Port      Type           Mode           VLAN    Status           Immediate Leave
-----
Fa0/1     NON MVR        Access         0       INACTIVE         DISABLED
```

This is an example of output from the **show mvr interface gigabitethernet0/1 members** command:

```
Switch# show mvr interface gigabitethernet0/1 members
239.255.0.0   vlan 202   DYNAMIC ACTIVE
239.255.0.1   vlan 202   DYNAMIC ACTIVE
239.255.0.2   vlan 202   DYNAMIC ACTIVE
239.255.0.3   vlan 203   DYNAMIC ACTIVE
239.255.0.4   vlan 203   DYNAMIC ACTIVE
239.255.0.5   vlan 203   DYNAMIC ACTIVE
```

**Related Commands**

Command	Description
<a href="#">mvr (global configuration)</a>	Enables and configures multicast VLAN registration on the switch.
<a href="#">mvr (interface configuration)</a>	Configures MVR ports.
<a href="#">show mvr</a>	Displays the global MVR configuration on the switch.
<a href="#">show mvr members</a>	Displays all receiver ports that are members of an MVR multicast group.

## show mvr members

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

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

<b>Syntax Description</b>	<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.
---------------------------	-------------------	---

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	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      Status    Members  VLAN  Membership
-----
239.1.1.1      ACTIVE   Fa0/1    1     Static
239.1.1.1      ACTIVE   Fa0/1    2000  Static
239.1.1.1      ACTIVE   Fa0/2    2     Static
239.1.1.1      ACTIVE   Fa0/2    3000  Static
239.1.1.2      ACTIVE   Fa0/1    1     Static
239.1.1.2      ACTIVE   Fa0/2    2     Static
```

<output truncated>

This is an example of output from the **show mvr members 239.255.0.2** command. It shows how to view the members of the IP multicast group 239.255.0.2:

```
Switch# show mvr members 239.255.0.2
239.255.0.2      ACTIVE           Gi0/1(d), Gi0/2(d), Gi0/3(d),
                  Gi0/4(d), Gi0/5(s)
```

Related Commands	Command	Description
	<a href="#">mvr (global configuration)</a>	Enables and configures multicast VLAN registration on the switch.
	<a href="#">mvr (interface configuration)</a>	Configures MVR ports.
	<a href="#">show mvr</a>	Displays the global MVR configuration on the switch.
	<a href="#">show mvr interface</a>	Displays the configured MVR interfaces, status of the specified interface, or all multicast groups to which the interface belongs when the <b>members</b> keyword is appended to the command.

# show pagp

Use the **show pagp** user EXEC command to display Port Aggregation Protocol (PAgP) channel-group information.

```
show pagp [channel-group-number] { counters | internal | neighbor }
```



## Note

PAgP is available only on network node interfaces (NNIs) or enhanced network interfaces (ENIs).

## Syntax Description

<i>channel-group-number</i>	(Optional) Number of the channel group. The range is 1 to 48.
<b>counters</b>	Display traffic information.
<b>internal</b>	Display internal information.
<b>neighbor</b>	Display neighbor information.

## Command Modes

User EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

You can enter any **show pagp** command to display the active channel-group information. To display the nonactive information, enter the **show pagp** command with a channel-group number.

## Examples

This is an example of output from the **show pagp 1 counters** command:

```
Switch> show pagp 1 counters
          Information          Flush
Port      Sent   Recv      Sent   Recv
-----
Channel group: 1
Gi0/1     45    42         0     0
  Gi0/2     45    41         0     0
```



This is an example of output from the **show pagp 1 internal** command:

```
Switch> show pagp 1 internal
Flags: S - Device is sending Slow hello. C - Device is in Consistent state.
      A - Device is in Auto mode.
Timers: H - Hello timer is running.      Q - Quit timer is running.
      S - Switching timer is running.    I - Interface timer is running.
```

Channel group 1

Port	Flags	State	Timers	Hello Interval	Partner Count	PAGP Priority	Learning Method	Group Ifindex
Gi0/1	SC	U6/S7	H	30s	1	128	Any	16
Gi0/2	SC	U6/S7	H	30s	1	128	Any	16

This is an example of output from the **show pagp 1 neighbor** command:

```
Switch> show pagp 1 neighbor
Flags: S - Device is sending Slow hello. C - Device is in Consistent state.
      A - Device is in Auto mode.      P - Device learns on physical port.
```

Channel group 1 neighbors

Port	Partner Name	Partner Device ID	Partner Port	Age	Partner Flags	Partner Group Cap.
Gi0/1	switch-p2	0002.4b29.4600	Gi0/1	9s	SC	10001
Gi0/2	switch-p2	0002.4b29.4600	Gi0/2	24s	SC	10001

#### Related Commands

Command	Description
<a href="#">clear pagp</a>	Clears PAGP channel-group information.

# show parser macro

Use the **show parser macro** user EXEC command to display the parameters for all configured macros or for one macro on the switch.

```
show parser macro [{brief | description [interface interface-id] | name macro-name}]
```

Syntax Description]	brief	(Optional) Display the name of each macro.
	<b>description</b> [interface <i>interface-id</i> ]	(Optional) Display all macro descriptions or the description of a specific interface.
	<b>name</b> <i>macro-name</i>	(Optional) Display information about a single macro identified by the macro name.

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

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

## Examples

This is a partial output example from the **show parser macro** command:

```
Switch# show parser macro
Total number of macros = 2
-----
Macro name : sample-macro1
Macro type : customizable
duplex full
speed auto
mdix auto
-----
Macro name : test1
Macro type : customizable
no shutdown
flowcontrol receive on
speed 100
-----
```

This is an example of output from the **show parser macro name** command:

```
Switch# show parser macro name sample-macro1
Macro name : sample-macro1
Macro type : customizable
duplex full
speed auto
mdix auto
```

This is an example of output from the **show parser macro brief** command:

```
Switch# show parser macro brief
customizable      : sample-macro1
customizable      : test1
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>macro apply</b>	Applies a macro on an interface or applies and traces a macro on an interface.
<b>macro description</b>	Adds a description about the macros that are applied to an interface.
<b>macro global</b>	Applies a macro on a switch or applies and traces a macro on a switch.
<b>macro global description</b>	Adds a description about the macros that are applied to the switch.
<b>macro name</b>	Creates a macro.
<b>show running-config</b>	Displays the operating configuration.

# show policer aggregate

Use the **show policer aggregate** user EXEC command to display quality of service (QoS) aggregate policer information for all aggregate policers or a specific policer.

```
show policer aggregate [aggregate-policer-name]
```

## Syntax Description

*aggregate-policer-name* (Optional) The name of the aggregate policer.

## Command Modes

User EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Examples

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

```
Switch> show policer aggregate my-policer
aggregate-policer: my-policer

    police cir 12000000 bc 5000
      conform-action transmit
      exceed-action set-cos-transmit cos table 67577

In use by policymap: pin
```

## Related Commands

Command	Description
<a href="#">police aggregate (policy-map class configuration)</a>	Applies an aggregate policer to multiple classes in the same policy map.
<a href="#">policer aggregate (global configuration)</a>	Creates an aggregate policer to police all traffic received on an interface.

## show policer cpu uni-eni

Use the **show policer cpu uni-eni** user EXEC command to display control-plane policer information for the user network interfaces (UNIs) and enhanced network interfaces (ENIs) on the switch, including frames dropped or the configured threshold rate for the control-plane security feature on the switch.

```
show policer cpu uni-eni { drop [interface interface-id] | rate }
```

Syntax Description	drop	(Optional) Display control-plane frame-drop count for all interfaces or the specified interface.
	<b>interface</b> <i>interface-id</i>	(Optional) Display the control-plane information for the specified physical interface.
	<b>rate</b>	(Optional) Display the configured threshold rate for CPU policers.

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

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** This command displays policer information that applies to UNIs and ENIs on the switch. Rate-limiting and policers are the same on both port types, except on ENIs on which a Layer 2 control protocol (CDP, STP, LLDP, LACP, or PAgP) has been enabled.

The output also displays if CPU protection has been disabled.

The **show policer cpu uni-eni drop** privileged EXEC command displays the number of accepted and dropped frames for all interfaces on the switch or for the specified interface.

The **show policer cpu uni-eni rate** command displays the CPU protection rate-limit threshold on the switch that was configured by entering the **policer cpu uni rate** global configuration command or the default rate of 16000 bits per second (bps).

**Examples**

This is an example of output from the **show policer cpu uni-eni drop** command.

```
Switch# show policer cpu uni-eni drop
=====
Port              In          Dropped
Name             Frames      Frames
Fa0/1             300         0
Fa0/2             0           0
Fa0/3             0           0
Fa0/4             0           0
Fa0/5             200         0
Fa0/6             0           0
Fa0/7             0           0
Fa0/8             0           0
Fa0/9             508055     325086
Fa0/10            0           0
Fa0/11            0           0
Fa0/12            0           0
Fa0/13            0           0
Fa0/14            0           0
Fa0/15            0           0
Fa0/16            0           0
Fa0/17            0           0
Fa0/18            0           0
Fa0/19            0           0
Fa0/20            0           0
Fa0/21            0           0
Fa0/22            0           0
Fa0/23            0           0
Fa0/24            0           0
Gi0/1             0           0
Gi0/2             0           0
drop-all         0           1849645
```

This is an example of the new output format for the **show policer cpu uni-eni drop interface** command:

```
Switch# show policer cpu uni-eni drop interface gigabitethernet 0/1
=====
Policer assigned for Gi0/2
=====
Protocols using this policer:
"VTP" "CISCO_L2" "KEEPALIVE" "SWITCH_IGMP" "SWITCH_L2PT"
Policer rate: 160000 bps
In frames: 48014
Drop frames: 28630
```

This is an example of output from the **show policer cpu uni-eni rate** command when the default rate is used.

```
Switch> show policer cpu uni-eni rate
CPU UNI/ENI port police rate = 160000 bps
```

This is an example of the show command output when CPU protection is disabled.

```
Switch# show policer cpu uni-eni rate
CPU Protection feature is not enabled
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">policer cpu uni</a>	Configures a CPU policer threshold rate for the switch or enables or disables CPU protection.
<a href="#">show platform policer cpu</a>	Displays allocated policer indexes and the corresponding features for all ports or the specified port.

# show policy-map

Use the **show policy-map** user EXEC command to display quality of service (QoS) policy maps, which define classification criteria for incoming and outgoing traffic and the actions to be performed on the classified traffic.

```
show policy-map [policy-map-name | interface [interface-id] [input | output] [class class-name]]
```

## Syntax Description

<i>policy-map-name</i>	(Optional) Display the specified policy-map name.
<b>class</b> <i>class-map-name</i>	(Optional) Display QoS policy actions for an individual class.
<b>interface</b> [ <i>interface-id</i> ] <b>[input   output]</b>	(Optional) Display information and statistics about policy maps applied to all ports or the specified port. If you specify a port, you can specify additional keywords. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <i>interface-id</i>—Display information about policy maps on the specified physical interface.</li> <li>• <b>input</b>—Display information about input policy maps on the switch or applied to the specified port.</li> <li>• <b>output</b>—Display the information about output policy-maps on the switch or applied to the specified port.</li> </ul>
<b>class</b> <i>class-name</i>	(Optional) Display policy-map statistics for an individual class.

## Command Modes

User EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Examples

This is an example of output from the **show policy-map interface** command:

```
Switch> show policy-map interface
GigabitEthernet0/1

Service-policy input: L3

Class-map: dscp-44 (match-all)
  0 packets
  Match: ip dscp 44
  police cir 68000000 bc 1000000
    conform-action set-dscp-transmit af41
    conform-action set-cos-transmit 3
    conform-action set-qos-transmit 18
    exceed-action set-dscp-transmit cs5
  conform: 0 (packets) 0 (bytes)
  exceed: 0 (packets) 0 (bytes)
  conform: 0 bps, exceed: 0 bps

Class-map: dscp-14 (match-any)
  0 packets
  Match: ip dscp af13 (14)
```



```

police cir 3000000 bc 93750 pir 5000000 be 156250
  conform-action set-prec-transmit 2
  conform-action set-cos-transmit precedence
  conform-action set-qos-transmit 12
  exceed-action set-cos-transmit precedence table tm-prec-to-cos
  exceed-action set-prec-transmit precedence
  violate-action set-cos-transmit 0
  violate-action set-dscp-transmit af13
conform: 0 (packets) 0 (bytes)
exceed: 0 (packets) 0 (bytes)
violate: 0 (packets) 0 (bytes)
conform: 0 bps, exceed: 0 bps, violate: 0 bps

Class-map: prec-5 (match-any)
  0 packets
  Match: ip precedence 5
  police cir 15000000 bc 468750 pir 16000000 be 500000
    conform-action transmit
    exceed-action set-dscp-transmit precedence
    violate-action set-cos-transmit dscp
conform: 0 (packets) 0 (bytes)
exceed: 0 (packets) 0 (bytes)
violate: 0 (packets) 0 (bytes)
conform: 0 bps, exceed: 0 bps, violate: 0 bps

Class-map: dscp-2 (match-all)
  0 packets
  Match: ip dscp 2
  police cir 34000000 bc 1000000 pir 37000000 be 1000000
    conform-action transmit
    exceed-action drop
    violate-action set-dscp-transmit af41
conform: 0 (packets) 0 (bytes)
exceed: 0 (packets) 0 (bytes)
violate: 0 (packets) 0 (bytes)
conform: 0 bps, exceed: 0 bps, violate: 0 bps

Class-map: prec-0 (match-any)
  0 packets
  Match: ip precedence 0
  police aggregate AP-L3-42m-2
conform: 0 (packets) 0 (bytes)
exceed: 0 (packets) 0 (bytes)
violate: 0 (packets) 0 (bytes)
conform: 0 bps, exceed: 0 bps, violate: 0 bps
NOTE: Policing statistics for a class configured with an aggregate policer are the
same for all classes in the policy-map configured with the same aggregate policer

```

<output truncated>

This is an example of output from the **show policy-map** command for a specific policy map:

```

Switch> show policy-map top2
Policy Map top2
  Class class-default
    shape average 11111124
    service-policy pout

```

This is an example of output from the **show policy-map** command for an output policy map:

```
Switch> show policy-map pout
Policy Map pout
  Class ip1
    priority
    police cir percent 10
      conform-action transmit
      exceed-action drop
    queue-limit 250
    queue-limit precedence 1 100
  Class ip2
    Average Rate Traffic Shaping
    cir 5%
  Class ip3
    bandwidth percent 10
    queue-limit 200
    queue-limit precedence 3 100
```

This is an example of output from the **show policy-map** command for an input policy map:

```
Switch> show policy-map pin-police
Policy Map pin-police
  Class ip1
    police cir 20000000 bc 625000
      conform-action transmit
      exceed-action drop
      violate-action drop
```

This is an example of output from the **show policy-map interface** command for an interface with a two-level output policy map applied:

```
Switch> show policy-map interface fastethernet0/3
FastEthernet0/3

Service-policy output: top2

Class-map: class-default (match-any)
  209871 packets
  Match: any
    56 packets
  Traffic Shaping
    Average Rate Traffic Shaping
    CIR 11111124 (bps)
  Output Queue:
    Tail Packets Drop: 195421

Service-policy : pout

Class-map: ip1 (match-all)
  9309 packets
  Match: ip precedence 1
  Priority
police cir 20000000 bc 625000
  conform-action transmit
  exceed-action drop
conform: 4916 (packets) exceed: 4393 (packets)
  Queue Limit
    queue-limit 250 (packets)
    queue-limit precedence 1 100 (packets)
  Output Queue:
    Max Tail Drop Threshold: 250
    Tail Packets Drop: 4393
```

```

Class-map: ip2 (match-all)
  0 packets
  Match: ip precedence 2
  Traffic Shaping
    Average Rate Traffic Shaping
    CIR 5%      555555 (bps)
  Output Queue:
    Max Tail Drop Threshold: 48
    Tail Packets Drop: 0

Class-map: ip3 (match-all)
  0 packets
  Match: ip precedence 3
  Bandwidth percent 10      1111110 (bps)
  Queue Limit
    queue-limit 200 (packets)
    queue-limit precedence 3 100 (packets)
  Output Queue:
    Max Tail Drop Threshold: 200
    Tail Packets Drop: 0

Class-map: class-default (match-any)
  200562 packets
  Match: any
    56 packets
  Output Queue:
    Tail Packets Drop: 191028

```

**Table 2-18** describes the fields in the **show policy-map interface** display. The fields in the table are grouped according to the relevant QoS feature.

**Table 2-18** *show policy-map interface Field Descriptions*

Field	Description
<b>Fields associated with classes or service policies</b>	
Service-policy input/output	Name of the input or output service policy applied to the specified interface.
Class-map	Class of traffic shown. Output appears for each configured class in the policy. The choice for implementing class matches (match-all or match-any) might also appear next to the traffic class.
packets	Number of packets identified as belonging to the traffic class.
Match	Match criteria specified for the class of traffic. This includes criteria such as class of service (CoS) value, IP precedence value, Differentiated Services Code Point (DSCP) value, access groups, and QoS groups.
<b>Fields associated with policing</b>	
police	Shown when the <b>police</b> command has been configured to enable traffic policing. Displays the specified committed information rate (CIR) and conform burst size (BC) used for policing packets.
conform-action	Displays the action to be taken on packets marked as conforming to a specified rate.
conform	Displays the number of packets marked as conforming to the specified rate.
exceed-action	Displays the actions to be taken on packets marked as exceeding a specified rate.

**Table 2-18** *show policy-map interface Field Descriptions (continued)*

Field	Description
exceed	Displays the number of packets marked as exceeding the specified rate.
violate-action	Displays the actions to be taken on packets marked as exceeding the maximum rate.
violate	Displays the number of packets marked as exceeding the maximum rate.
<b>Fields associated with queuing</b>	
Queue Limit	Queue size configured for the class in number of packets.
Output Queue	The queue created for this class of traffic.
Tail packets dropped	The number of packets dropped when the mean queue depth is greater than the maximum threshold value.
<b>Fields associated with traffic scheduling</b>	
Traffic shaping	The rate used for shaping traffic.
Bandwidth	Bandwidth configured for this class in kbps or a percentage.
Priority	Indicates that this class is configured for priority queuing.

**Related Commands**

Command	Description
<a href="#">policy-map</a>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.

# show port-security

Use the **show port-security** privileged EXEC command to display port-security settings for an interface or for the switch.

**show port-security** [**interface** *interface-id*] [**address** | **vlan**]

## Syntax Description

<b>interface</b> <i>interface-id</i>	(Optional) Display port security settings for the specified interface. Valid interfaces include physical ports (including type, module, and port number).
<b>address</b>	(Optional) Display all secure MAC addresses on all ports or a specified port.
<b>vlan</b>	(Optional) Display port security settings for all VLANs on the specified interface. This keyword is visible only on interfaces that have the switchport mode set to <b>trunk</b> .

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

If you enter the command without keywords, the output includes the administrative and operational status of all secure ports on the switch.

If you enter an *interface-id*, the command displays port security settings for the interface.

If you enter the **address** keyword, the command displays the secure MAC addresses for all interfaces and the aging information for each secure address.

If you enter an *interface-id* and the **address** keyword, the command displays all the MAC addresses for the interface with aging information for each secure address. You can also use this command to display all the MAC addresses for an interface even if you have not enabled port security on it.

If you enter the **vlan** keyword, the command displays the configured maximum and the current number of secure MAC addresses for all VLANs on the interface. This option is visible only on interfaces that have the switchport mode set to **trunk**.

**Examples**

This is an example of the output from the **show port-security** command:

```
Switch# show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
              (Count)          (Count)      (Count)
-----
      Gi0/1          1              0              0              Shutdown
-----
Total Addresses in System (excluding one mac per port) : 1
Max Addresses limit in System (excluding one mac per port) : 6272
```

This is an example of output from the **show port-security interface interface-id** command:

```
Switch# show port-security interface gigabitethernet0/1
Port Security : Enabled
Port status : SecureUp
Violation mode : Shutdown
Maximum MAC Addresses : 1
Total MAC Addresses : 0
Configured MAC Addresses : 0
Aging time : 0 mins
Aging type : Absolute
SecureStatic address aging : Disabled
Security Violation count : 0
```

This is an example of output from the **show port-security address** command:

```
Switch# show port-security address
Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
      (mins)
-----
      1    0006.0700.0800  SecureConfigured   Gi0/2    1
-----
Total Addresses in System (excluding one mac per port) : 1
Max Addresses limit in System (excluding one mac per port) : 6272
```

This is an example of output from the **show port-security interface gigabitethernet0/2 address** command:

```
Switch# show port-security interface gigabitethernet0/2 address
Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
      (mins)
-----
      1    0006.0700.0800  SecureConfigured   Gi0/2    1
-----
Total Addresses: 1
```

This is an example of output from the **show port-security interface interface-id vlan** command:

```
Switch# show port-security interface gigabitethernet0/2 vlan
Default maximum: not set, using 5120
VLAN  Maximum  Current
    5    default    1
    10   default    54
    11   default    101
    12   default    101
    13   default    201
    14   default    501
```

Related Commands	Command	Description
	<a href="#">clear port-security</a>	Deletes from the MAC address table a specific type of secure address or all the secure addresses on the switch or an interface.
	<a href="#">switchport port-security</a>	Enables port security on a port, restricts the use of the port to a user-defined group of stations, and configures secure MAC addresses.

# show port-type

Use the **show port-type** privileged EXEC command to display interface type information for the Cisco ME switch.

**show port-type [eni | nni | uni]**

## Syntax Description

<b>eni</b>	Enhanced network interface.
<b>nni</b>	Network node interface.
<b>uni</b>	User network interface.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

If you enter the command without keywords, the output includes the interface type information for all ports on the switch. If you specify the port type (**eni**, **nni**, or **uni**), the output includes information for the specified port type.

## Examples

This is an example of output from the **show port-type** command with no keywords:

```
Switch# show port-type
Port      Name              Vlan      Port Type
-----
Fa0/1    User Network Interface (uni)
Fa0/2    User Network Interface (uni)
Fa0/3    User Network Interface (uni)
Fa0/4    User Network Interface (uni)
Fa0/5    User Network Interface (uni)
Fa0/6    User Network Interface (uni)
Fa0/7    User Network Interface (uni)
Fa0/8    User Network Interface (uni)
Fa0/9    User Network Interface (uni)
Fa0/10   User Network Interface (uni)
Fa0/11   User Network Interface (uni)
Fa0/12   User Network Interface (uni)
Fa0/13   User Network Interface (uni)
Fa0/14   User Network Interface (uni)
Fa0/15   User Network Interface (uni)
Fa0/16   User Network Interface (uni)
Fa0/17   routed           User Network Interface (uni)
Fa0/18   1                User Network Interface (uni)
Fa0/19   1                User Network Interface (uni)
Fa0/20   1                User Network Interface (uni)
Fa0/21   1                User Network Interface (uni)
Fa0/22   1                User Network Interface (uni)
Fa0/23   10              User Network Interface (uni)
Fa0/24   10              User Network Interface (uni)
```



```

Gi0/1          1          Network Node Interface (nni)
Gi0/2          1          Network Node Interface (nni)

```

This is an example of output from the **show port-type** command using keywords:

```

Switch# show port-type nni | exclude GigabitEthernet0/1
Port      Name      Vlan      Port Type
-----
Gi0/2          1          Network Node Interface (nni)

```

#### Related Commands

Command	Description
<a href="#">port-type</a>	Changes the interface type for a specific port.

# show rep topology

Use the **show rep topology** User EXEC command 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.

**show rep topology** [*segment segment\_id*] [**archive**] [**detail**]

## Syntax Description

<b>segment-id</b>	(Optional) Display REP topology information for the specified segment. The ID range is from 1 to 1024.
<b>archive</b>	(Optional) Display the previous topology of the segment. This keyword can be useful for troubleshooting a link failure.
<b>detail</b>	(Optional) Display detailed REP topology information.

## Command Modes

User EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

In the **show rep topology** command output, ports configured as edge no-neighbor are designated with an asterisk (\*) in front of *Pri* or *Sec*. In the output of the **show rep topology detail** command, *No-Neighbor* is spelled out.

The output of this command is also included in the **show tech-support** privileged EXEC command output.

## Examples

This is a sample output from the **show rep topology segment** privileged EXEC command:

```
Switch # show rep topology segment 1
REP Segment 1
BridgeName      PortName      Edge Role
-----
sw1_multseg_3750 Gi1/1/1      Pri  Alt
sw3_multseg_3400 Gi0/13              Open
sw3_multseg_3400 Gi0/14              Alt
sw4_multseg_3400 Gi0/13              Open
sw4_multseg_3400 Gi0/14              Open
sw5_multseg_3400 Gi0/13              Open
sw5_multseg_3400 Gi0/14              Open
sw2_multseg_3750 Gi1/1/2              Open
sw2_multseg_3750 Gi1/1/1              Open
sw1_multseg_3750 Gi1/1/2      Sec  Open
```

This is a sample output from the **show rep topology** command when the edge ports are configured to have no REP neighbor:

```
Switch # show rep topology
REP Segment 2
BridgeName      PortName      Edge Role
```

```

-----
sw8-ts8-51      Gi0/2      Pri*  Open
sw9-ts11-50    Gi1/0/4    Open
sw9-ts11-50    Gi1/0/2    Open
sw1-ts11-45    Gi0/2      Alt
sw1-ts11-45    Po1        Open
sw8-ts8-51     Gi0/1      Sec*  Open

```

This example shows output from the **show rep topology detail** command:

```

Switch# show rep topology detail
REP Segment 2
repc_2_24ts, Fa0/2 (Primary Edge)
  Alternate Port, some vlans blocked
  Bridge MAC: 0019.e714.5380
  Port Number: 004
  Port Priority: 080
  Neighbor Number: 1 / [-10]
repc_3_12cs, Gi0/1 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 001a.a292.3580
  Port Number: 001
  Port Priority: 000
  Neighbor Number: 2 / [-9]
repc_3_12cs, Po10 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 001a.a292.3580
  Port Number: 080
  Port Priority: 000
  Neighbor Number: 3 / [-8]
repc_4_12cs, Po10 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 001a.a19d.7c80
  Port Number: 080
  Port Priority: 000
  Neighbor Number: 4 / [-7]
repc_4_12cs, Gi0/2 (Intermediate)
  Alternate Port, some vlans blocked
  Bridge MAC: 001a.a19d.7c80
  Port Number: 002
  Port Priority: 040
  Neighbor Number: 5 / [-6]

```

<output truncated>

This example shows output from the **show rep topology segment archive** command:

```

Switch# show rep topology segment 1 archive
REP Segment 1
BridgeName      PortName      Edge Role
-----
sw1_multseg_3750 Gi1/1/1      Pri  Open
sw3_multseg_3400 Gi0/13       Open
sw3_multseg_3400 Gi0/14       Open
sw4_multseg_3400 Gi0/13       Open
sw4_multseg_3400 Gi0/14       Open
sw5_multseg_3400 Gi0/13       Open
sw5_multseg_3400 Gi0/14       Open
sw2_multseg_3750 Gi1/1/2      Alt
sw2_multseg_3750 Gi1/1/1      Open
sw1_multseg_3750 Gi1/1/2      Sec  Open

```

■ show rep topology

Related Commands	Command	Description
	<a href="#">rep segment</a>	Enables REP on an interface and assigns a segment ID. This command is also used to configure a port as an edge port, a primary edge port, or a preferred port.

# show sdm prefer

Use the **show sdm prefer** privileged EXEC command to display the Switch Database Management (SDM) templates that can be used to allocate system resources for a particular feature, or use the command without a keyword to display the template in use.

```
show sdm prefer [default | dual-ipv4-and-ipv6 {default | routing | vlan} | layer-2]
```



## Note

The **default** and **dual-ipv4-and-ipv6** keywords are visible only when the metro IP access image is installed on the switch.

## Syntax Description

<b>default</b>	(Optional) Display the template that balances system resources among features.
<b>dual-ipv4-and-ipv6</b> { <b>default</b>   <b>routing</b>   <b>vlan</b> }	(Optional) Display the dual templates that support both IPv4 and IPv6. <ul style="list-style-type: none"> <li>• <b>default</b>—Display the default dual template configuration.</li> <li>• <b>routing</b>—Display the routing dual template configuration.</li> <li>• <b>vlan</b>—Display the VLAN dual template configuration.</li> </ul>
<b>layer-2</b>	(Optional) Display resource allocations for the template that supports Layer 2 features and does not support routing.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

When you change the SDM template by using the **sdm prefer** global configuration command, you must reload the switch for the configuration to take effect. If you enter the **show sdm prefer** command before you enter the **reload** privileged EXEC command, the **show sdm prefer** command shows the template currently in use and the template that will become active after a reload.

The numbers displayed represent an approximate maximum number for each feature resource. The actual number might vary, depending on the actual number of other features configured.

## Examples

This is an example of output from the **show sdm prefer** command, displaying the template in use:

```
Switch# show sdm prefer
The current template is ''layer-2'' template.
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:          8K
number of IPv4 IGMP groups:              1K
number of IPv4 multicast routes:         0
```

## ■ show sdm prefer

```

number of unicast IPv4 routes:          0
number of IPv4 policy based routing aces: 0
number of IPv4/MAC qos aces:          512
number of IPv4/MAC security aces:      1K

```

This is an example of output from the **show sdm prefer default** command:

```

Switch# show sdm prefer default
"default" template:
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:        5K
  number of IPv4 IGMP groups + multicast routes: 1K
  number of IPv4 unicast routes:        9K
    number of directly-connected IPv4 hosts: 5K
    number of indirect IPv4 routes:      4K
  number of IPv4 policy based routing aces: 512
  number of IPv4/MAC qos aces:          512
  number of IPv4/MAC security aces:      1K

```

This is an example of output from the **show sdm prefer dual-ipv4-and-ipv6 routing** command:

```

Switch# show sdm prefer dual-ipv4-and-ipv6 routing
"desktop IPv4 and IPv6 routing" template:
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:        1.5K
number of IPv4 IGMP groups + multicast routes: 1K
number of IPv4 unicast routes:        2.75K
  number of directly-connected IPv4 hosts: 1.5K
  number of indirect IPv4 routes:      1.25K
number of IPv6 multicast groups:      1.125k
number of directly-connected IPv6 addresses: 1.5K
number of indirect IPv6 unicast routes: 1.25K
number of IPv4 policy based routing aces: 0.25K
number of IPv4/MAC qos aces:          0.75K
number of IPv4/MAC security aces:      0.5K
number of IPv6 policy based routing aces: 0.25K
number of IPv6 qos aces:              0.5K
number of IPv6 security aces:          0.5K

```

---

**Related Commands**

Command	Description
<a href="#">sdm prefer</a>	Sets the SDM template to maximize resources for Layer 2 functionality or to the default template.

---

# show spanning-tree

Use the **show spanning-tree** user EXEC command to display spanning-tree state information.

```
show spanning-tree [bridge-group | active [detail] | blockedports | bridge | detail [active] |
inconsistentports | interface interface-id | mst | pathcost method | root | summary [totals] |
vlan vlan-id]
```

```
show spanning-tree bridge-group [active [detail] | blockedports | bridge | detail [active] |
inconsistentports | interface interface-id | root | summary]
```

```
show spanning-tree vlan vlan-id [active [detail] | blockedports | bridge | detail [active] |
inconsistentports | interface interface-id | root | summary]
```

```
show spanning-tree {vlan vlan-id | bridge-group} bridge [address | detail | forward-time |
hello-time | id | max-age | priority [system-id] | protocol]
```

```
show spanning-tree {vlan vlan-id | bridge-group} root [address | cost | detail | forward-time |
hello-time | id | max-age | port | priority [system-id]
```

```
show spanning-tree interface interface-id [active [detail] | cost | detail [active] | inconsistency |
portfast | priority | rootcost | state]
```

```
show spanning-tree mst [configuration [digest]] | [instance-id [detail | interface interface-id
detail]]
```

## Syntax Description

<i>bridge-group</i>	(Optional) Specify the bridge group number. The range is 1 to 255.
<b>active</b> [ <b>detail</b> ]	(Optional) Display spanning-tree information only on active interfaces (available only in privileged EXEC mode).
<b>blockedports</b>	(Optional) Display blocked port information (available only in privileged EXEC mode).
<b>bridge</b> [ <b>address</b>   <b>detail</b>   <b>forward-time</b>   <b>hello-time</b>   <b>id</b>   <b>max-age</b>   <b>priority</b> [ <b>system-id</b> ]   <b>protocol</b> ]	(Optional) Display status and configuration of this switch (optional keywords available only in privileged EXEC mode).
<b>detail</b> [ <b>active</b> ]	(Optional) Display a detailed summary of interface information ( <b>active</b> keyword available only in privileged EXEC mode).
<b>inconsistentports</b>	(Optional) Display inconsistent port information (available only in privileged EXEC mode).
<b>interface</b> <i>interface-id</i> [ <b>active</b> [ <b>detail</b> ]   <b>cost</b>   <b>detail</b> [ <b>active</b> ]   <b>inconsistency</b>   <b>portfast</b>   <b>priority</b>   <b>rootcost</b>   <b>state</b> ]	(Optional) Display spanning-tree information for the specified interface (all options except <b>portfast</b> and <b>state</b> available only in privileged EXEC mode). Enter each interface separated by a space. Ranges are not supported. Valid interfaces include physical network node interfaces (NNIs), enhanced network interfaces (ENIs), VLANs, and NNI or ENI port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 48.
<b>Note</b>	Spanning Tree Protocol (STP) is not supported on user node interfaces (UNIs). If you enter a UNI interface ID, no spanning-tree information is displayed.

<b>mst</b> [ <b>configuration</b>   <b>digest</b> ]] [ <i>instance-id</i>   <b>detail</b>   <b>interface</b> <i>interface-id</i> [ <b>detail</b> ]]	<p>(Optional) Display the multiple spanning-tree (MST) region configuration and status (available only in privileged EXEC mode).</p> <p>The keywords have these meanings:</p> <ul style="list-style-type: none"> <li>• <b>digest</b>—(Optional) Display the MD5 digest included in the current MST configuration identifier (MSTCI). Two separate digests, one for standard and one for prestandard switches, appear (available only in privileged EXEC mode).</li> </ul> <p>The terminology was updated for the implementation of the IEEE standard, and the <i>txholdcount</i> field was added.</p> <p>The new master role appears for boundary ports.</p> <p>The word <i>pre-standard</i> or <i>Pre-STD</i> appears when an IEEE standard bridge sends prestandard BPDUs on a port.</p> <p>The word <i>pre-standard (config)</i> or <i>Pre-STD-Cf</i> appears when a port has been configured to send prestandard BPDUs and no prestandard BPDUs has been received on that port.</p> <p>The word <i>pre-standard (rcvd)</i> or <i>Pre-STD-Rx</i> appears when a prestandard BPDUs has been received on a port that has not been configured to send prestandard BPDUs.</p> <p>A <i>dispute</i> flag appears when a designated port receives inferior designated information until the port returns to the forwarding state or ceases to be designated.</p> <ul style="list-style-type: none"> <li>• <i>instance-id</i>—You can specify a single instance ID, a range of IDs separated by a hyphen, or a series of IDs separated by a comma. The range is 1 to 4094. The display shows the number of currently configured instances.</li> <li>• <b>interface</b> <i>interface-id</i>—(Optional) Valid interfaces include VLANs, physical NNIs and NNI port channels, and physical ENIs and ENI port channels. STP is not supported on UNIs. The VLAN range is 1 to 4094. The port-channel range is 1 to 48.</li> <li>• <b>detail</b>—(Optional) Display detailed information for the instance or interface.</li> </ul>
<b>pathcost method</b>	(Optional) Display the default path cost method (available only in privileged EXEC mode).
<b>root</b> [ <b>address</b>   <b>cost</b>   <b>detail</b>   <b>forward-time</b>   <b>hello-time</b>   <b>id</b>   <b>max-age</b>   <b>port</b>   <b>priority</b> [ <b>system-id</b> ]]	(Optional) Display root switch status and configuration (all keywords available only in privileged EXEC mode).
<b>summary</b> [ <b>totals</b> ]	(Optional) Display a summary of port states or the total lines of the spanning-tree state section.
<b>vlan</b> <i>vlan-id</i> [ <b>active</b>   <b>detail</b> ]   <b>backbonefast</b>   <b>blockedports</b>   <b>bridge</b> [ <b>address</b>   <b>detail</b> ]   <b>forward-time</b>   <b>hello-time</b>   <b>id</b>   <b>max-age</b>   <b>priority</b> [ <b>system-id</b> ]   <b>protocol</b> ]	(Optional) Display spanning-tree information for the specified VLAN (some keywords available only in privileged EXEC mode). You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.



**Command Modes** User EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** STP is not supported on UNIs. Valid spanning-tree information is available only for NNIs or ENIs. If the *vlan-id* variable is omitted, the command applies to the spanning-tree instance for all VLANs.

**Examples** This is an example of output from the **show spanning-tree active** command:

```
Switch# show spanning-tree active
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID      Priority    32768
              Address    0001.42e2.cdd0
              Cost      3038
              Port      24 (GigabitEthernet0/1)
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID    Priority    49153 (priority 49152 sys-id-ext 1)
              Address    0003.fd63.9580
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300
  Uplinkfast   enabled

Interface      Role Sts Cost      Prio.Nbr Type
-----
Gi0/1          Root FWD 3019     128.24  P2p
<output truncated>
```

This is an example of output from the **show spanning-tree detail** command:

```
Switch# show spanning-tree detail
VLAN0001 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 49152, sysid 1, address 0003.fd63.9580
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32768, address 0001.42e2.cdd0
  Root port is 24 (GigabitEthernet0/1), cost of root path is 3038
  Topology change flag not set, detected flag not set
  Number of topology changes 0 last change occurred 1d16h ago
  Times: hold 1, topology change 35, notification 2
         hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300
  Uplinkfast enabled

Port 1 (GigabitEthernet0/1) of VLAN0001 is forwarding
  Port path cost 3019, Port priority 128, Port Identifier 128.24.
  Designated root has priority 32768, address 0001.42e2.cdd0
  Designated bridge has priority 32768, address 00d0.bbf5.c680
  Designated port id is 128.25, designated path cost 19
  Timers: message age 2, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  Link type is point-to-point by default
  BPDU: sent 0, received 72364
<output truncated>
```

This is an example of output from the **show spanning-tree interface *interface-id*** command:

```
Switch# show spanning-tree interface gigabitethernet0/1
Vlan          Role Sts Cost      Prio.Nbr Type
-----
VLAN0001      Root FWD 3019      128.24 P2p
```

This is an example of output from the **show spanning-tree summary** command:

```
Switch# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
EtherChannel misconfiguration guard is enabled
Extended system ID is enabled
Portfast is disabled by default
PortFast BPDU Guard is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard is disabled by default
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.

This is an example of output from the **show spanning-tree mst configuration** command:

```
Switch# show spanning-tree mst configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
-----
0         1-9,21-4094
1         10-20
-----
```

This is an example of output from the **show spanning-tree mst configuration digest** command:

```
Switch# show spanning-tree mst configuration
% Switch is not in mst mode
Name      []
Revision  0      Instances configured 1
Digest    0xAC36177F50283CD4B83821D8AB26DE62
Pre-std Digest 0xBB3B6C15EF8D089BB55ED10D24DF44DE
```

This is an example of output from the **show spanning-tree mst interface *interface-id*** command:

```
Switch# show spanning-tree mst interface gigabitethernet0/1
GigabitEthernet0/1 of MST00 is root forwarding
Edge port: no (default) port guard : none (default)
Link type: point-to-point (auto) bpdu filter: disable (default)
Boundary : boundary (STP) bpdu guard : disable (default)
Bpdus sent 5, received 74

Instance role state cost prio vlans mapped
0 root FWD 200000 128 1,12,14-4094
```

This is an example of output from the **show spanning-tree mst 0** command:

```
Switch# show spanning-tree mst 0
##### MST00          vlans mapped: 1-9,21-4094
Bridge      address 0002.4b29.7a00  priority 32768 (32768 sysid 0)
Root       address 0001.4297.e000  priority 32768 (32768 sysid 0)
port      Gi0/1          path cost 200038
IST master *this switch
Operational hello time 2, forward delay 15, max age 20, max hops 20
Configured  hello time 2, forward delay 15, max age 20, max hops 20
```

Interface	role	state	cost	prio	type
GigabitEthernet0/1	root	FWD	200000	128	P2P bound(STP)
GigabitEthernet0/2	desg	FWD	200000	128	P2P bound(STP)
Port-channel1	desg	FWD	200000	128	P2P bound(STP)

■ show spanning-tree

Related Commands	Command	Description
	<b>clear spanning-tree counters</b>	Clears the spanning-tree counters.
	<b>clear spanning-tree detected-protocols</b>	Restarts the protocol migration process.
	<b>spanning-tree bpdudfilter</b>	Prevents an interface from sending or receiving bridge protocol data units (BPDUs).
	<b>spanning-tree bpduguard</b>	Puts an interface in the error-disabled state when it receives a BPDU.
	<b>spanning-tree cost</b>	Sets the path cost for spanning-tree calculations.
	<b>spanning-tree extend system-id</b>	Enables the extended system ID feature.
	<b>spanning-tree guard</b>	Enables the root guard or the loop guard feature for all the VLANs associated with the selected interface.
	<b>spanning-tree link-type</b>	Overrides the default link-type setting for rapid spanning-tree transitions to the forwarding state.
	<b>spanning-tree loopguard default</b>	Prevents alternate or root ports from becoming the designated port because of a failure that leads to a unidirectional link.
	<b>spanning-tree mst configuration</b>	Enters multiple spanning-tree (MST) configuration mode through which the MST region configuration occurs.
	<b>spanning-tree mst cost</b>	Sets the path cost for MST calculations.
	<b>spanning-tree mst forward-time</b>	Sets the forward-delay time for all MST instances.
	<b>spanning-tree mst hello-time</b>	Sets the interval between hello BPDUs sent by root switch configuration messages.
	<b>spanning-tree mst max-age</b>	Sets the interval between messages that the spanning tree receives from the root switch.
	<b>spanning-tree mst max-hops</b>	Sets the number of hops in an MST region before the BPDU is discarded and the information held for an interface is aged.
	<b>spanning-tree mst port-priority</b>	Configures an interface priority.
	<b>spanning-tree mst priority</b>	Configures the switch priority for the specified spanning-tree instance.
	<b>spanning-tree mst root</b>	Configures the MST root switch priority and timers based on the network diameter.
	<b>spanning-tree port-priority</b>	Configures an interface priority.
	<b>spanning-tree portfast (global configuration)</b>	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled interfaces or enables the Port Fast feature on all nontrunking interfaces.
	<b>spanning-tree portfast (interface configuration)</b>	Enables the Port Fast feature on an interface and all its associated VLANs.
	<b>spanning-tree vlan</b>	Configures spanning tree on a per-VLAN basis.

# show storm-control

Use the **show storm-control** user EXEC command to display broadcast, multicast, or unicast storm control settings on the switch or on the specified interface or to display storm-control history.

**show storm-control** [*interface-id*] [**broadcast** | **multicast** | **unicast**]

Syntax Description	
<i>interface-id</i>	(Optional) Interface ID for the physical port (including type, module, and port number).
<b>broadcast</b>	(Optional) Display broadcast storm threshold setting.
<b>multicast</b>	(Optional) Display multicast storm threshold setting.
<b>unicast</b>	(Optional) Display unicast storm threshold setting.

**Command Modes** User EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** When you enter an *interface-id*, the storm control thresholds appear for the specified interface. If you do not enter an *interface-id*, settings appear for one traffic type for all ports on the switch. If you do not enter a traffic type, settings appear for broadcast storm control.

**Examples** This is an example of a partial output from the **show storm-control** command when no keywords are entered. Because no traffic-type keyword was entered, the broadcast storm control settings appear.

```
Switch> show storm-control
Interface   Filter State  Upper      Lower      Current
-----
Gi0/1      Forwarding   20 pps    10 pps     5 pps
Gi0/2      Forwarding   50.00%    40.00%    0.00%
<output truncated>
```

This is an example of output from the **show storm-control** command for a specified interface. Because no traffic-type keyword was entered, the broadcast storm control settings appear.

```
Switch> show storm-control gigabitethernet 0/1
Interface  Filter State  Upper      Lower      Current
-----  -
Gi0/1     Forwarding    20 pps     10 pps     5 pps
```

Table 2-19 describes the fields in the **show storm-control** display.

**Table 2-19** show storm-control Field Descriptions

Field	Description
Interface	Displays the ID of the interface.
Filter State	Displays the status of the filter: <ul style="list-style-type: none"> <li>Blocking—Storm control is enabled, and a storm has occurred.</li> <li>Forwarding—Storm control is enabled, and no storms have occurred.</li> <li>Inactive—Storm control is disabled.</li> </ul>
Upper	Displays the rising suppression level as a percentage of total available bandwidth in packets per second or in bits per second.
Lower	Displays the falling suppression level as a percentage of total available bandwidth in packets per second or in bits per second.
Current	Displays the bandwidth usage of broadcast traffic or the specified traffic type (broadcast, multicast, or unicast) as a percentage of total available bandwidth. This field is only valid when storm control is enabled.

#### Related Commands

Command	Description
<a href="#">storm-control</a>	Sets the broadcast, multicast, or unicast storm control levels for the switch.

# show system mtu

Use the **show system mtu** privileged EXEC command to display the global maximum transmission unit (MTU) or maximum packet size set for the switch.

**show system mtu**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** If you have used the **system mtu** or **system mtu jumbo** global configuration command to change the MTU setting, the new setting does not take effect until you reset the switch.

The system MTU refers to ports operating at 10/100 Mb/s; the system jumbo MTU refers to Gigabit ports; the routing MTU is the MTU for routed packets.

**output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

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

```
Switch# show system mtu

System MTU size is 1500 bytes
System Jumbo MTU size is 5000 bytes
System Alternate MTU size is 2000 bytes
Routing MTU size is 1500 bytes
```

This is an example of output when you have defined an alternate MTU size, but not reloaded the switch:

```
Switch# show system mtu

System MTU size is 1500 bytes
System Jumbo MTU size is 5000 bytes
System Alternate MTU size is 1500 bytes
On next reload, System Alternate MTU will be 2000 bytes
Routing MTU size is 1500 bytes
```

Related Commands	Command	Description
	<b>show interface interface-id mtu</b>	Displays the MTU setting on the specified interface.
	<b>system mtu</b>	Sets the MTU size for the Fast Ethernet or Gigabit Ethernet ports, or set an alternate MTU size to be applied to specific interfaces.

# show table-map

Use the **show table-map** user EXEC command to display quality of service (QoS) table-map information about all configured table maps or the specified table map.

**show table-map** [*table-map-name*]

<b>Syntax Description</b>	<i>table-map-name</i> (Optional) The name of the table map.				
<b>Command Modes</b>	User EXEC				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(44)EY</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(44)EY	This command was introduced.
Release	Modification				
12.2(44)EY	This command was introduced.				

## Examples

This is an example of output from the **show table-map** command:

```
Switch> show table-map
tandoori_1>show table-map
  Table Map abc
    default copy

  Table Map cos2dscp
    from 2 to 16
    default copy

  Table Map cos2cos
    from 2 to 5
    from 3 to 6
    default 7

  Table Map cos2cos10
    default copy

  Table Map cos=cos
    default copy
```

This is an example of output from the **show table-map** command for a specific table map name:

```
Switch> show table-map tm

  Table Map tm
    from 1 to 62
    from 2 to 63
    default ignore
```

Related Commands	Command	Description
	<a href="#">table-map</a>	Creates quality of service (QoS) mapping tables, such as CoS to DSCP, and so on.



# show uddld

Use the **show uddld** user EXEC command to display UniDirectional Link Detection (UDLD) administrative and operational status for all ports or the specified port.

**show uddld** [*interface-id*]

<b>Syntax Description</b>	<i>interface-id</i>	(Optional) ID of the interface and port number. Valid interfaces include physical ports and VLANs. The VLAN range is 1 to 4094.
---------------------------	---------------------	---

<b>Command Modes</b>	User EXEC
----------------------	-----------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

<b>Usage Guidelines</b>	If you do not enter an <i>interface-id</i> , administrative and operational UDLD status for all interfaces appear.
-------------------------	--

**Examples** This is an example of output from the **show uddld interface-id** command. For this display, UDLD is enabled on both ends of the link, and UDLD detects that the link is bidirectional. [Table 2-20](#) describes the fields in this display.

```
Switch> show uddld gigabitethernet0/1
Interface gi0/1
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single Neighbor detected
Message interval: 60
Time out interval: 5
  Entry 1
    Expiration time: 146
    Device ID: 1
    Current neighbor state: Bidirectional
    Device name: Switch-A
    Port ID: Gi0/1
    Neighbor echo 1 device: Switch-B
    Neighbor echo 1 port: Gi0/2
    Message interval: 5
    CDP Device name: Switch-A
```

**Table 2-20** *show uddl Field Descriptions*

Field	Description
Interface	The interface on the local device configured for UDLD.
Port enable administrative configuration setting	How UDLD is configured on the port. If UDLD is enabled or disabled, the port enable configuration setting is the same as the operational enable state. Otherwise, the enable operational setting depends on the global enable setting.
Port enable operational state	Operational state that shows whether UDLD is actually running on this port.
Current bidirectional state	The bidirectional state of the link. An unknown state appears if the link is down or if it is connected to an UDLD-incapable device. A bidirectional state appears if the link is a normal two-way connection to a UDLD-capable device. All other values mean miswiring.
Current operational state	The current phase of the UDLD state machine. For a normal bidirectional link, the state machine is most often in the Advertisement phase.
Message interval	How often advertisement messages are sent from the local device. Measured in seconds.
Time out interval	The time period, in seconds, that UDLD waits for echoes from a neighbor device during the detection window.
Entry 1	Information from the first cache entry, which contains a copy of echo information received from the neighbor.
Expiration time	The amount of time in seconds remaining before this cache entry is aged out.
Device ID	The neighbor device identification.
Current neighbor state	The neighbor's current state. If both the local and neighbor devices are running UDLD normally, the neighbor state and local state should be bidirectional. If the link is down or the neighbor is not UDLD-capable, no cache entries appear.
Device name	The device name or the system serial number of the neighbor. The system serial number appears if the device name is not set or is set to the default (Switch).
Port ID	The neighbor port ID enabled for UDLD.
Neighbor echo 1 device	The device name of the neighbors' neighbor from which the echo originated.
Neighbor echo 1 port	The port number ID of the neighbor from which the echo originated.
Message interval	The rate, in seconds, at which the neighbor is sending advertisement messages.
CDP device name	The CDP device name or the system serial number. The system serial number appears if the device name is not set or is set to the default (Switch).

Related Commands	Command	Description
	<b>uddl</b>	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
	<b>uddl port</b>	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the <b>uddl</b> global configuration command.
	<b>uddl reset</b>	Resets all interfaces shutdown by UDLD and permits traffic to begin passing through them again.

# show version

Use the **show version** user EXEC command to display version information for the hardware and firmware.

## show version

**Syntax Description** This command has no arguments or keywords.

**Command Modes** User EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

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



**Note** Though visible in the **show version** output, the *configuration register* information is not supported on the switch.

```
Switch> show version
Cisco IOS Software, MEAP Software (MEAP-IPSERVICES-M), Experimental Version 12.2
(20050712:084347) [teresang-meap-bug-fix 109]
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Sun 17-Jul-05 13:19 by teresang
```

```
ROM: Bootstrap program is C3750 boot loader
BOOTLDR: ME3400 Boot Loader (me3400-HBOOT-M), Version 12.2 [mbutts-meap2 103]
```

```
tandoori_1 uptime is 1 day, 2 hours, 49 minutes
System returned to ROM by power-on
System image file is "flash:image"
```

```
cisco ME-3440-24T-FA (PowerPC405) processor with 118784K/12280K bytes of memory.
```

```
Processor board ID FSJC0407862
Last reset from power-on
Target IOS Version 12.2(25)SE
3 Virtual Ethernet interfaces
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.
```

```
512K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:0B:FC:FF:32:80
Power supply part number        : 341-0149-01
Motherboard serial number       : FHH0848001R
Power supply serial number      : DTH0450000T
System serial number            : FSJC0407862
Top Assembly Part Number       : 800-26552-01
Top Assembly Revision Number   : 05
```

Hardware Board Revision Number : 0x01

Switch	Ports	Model	SW Version	SW Image
-----	-----	-----	-----	-----
* 1	26	ME-3440-24T-FA	12.2(20050712:084347)	MEAP-IPSERVICES-M

Configuration register is 0xF

# show vlan

Use the **show vlan** user EXEC command to display the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) on the switch.

```
show vlan [access-map | brief | dot1q tag native | filter | id vlan-id | internal usage | mtu | name
          vlan-name | private-vlan [type] | remote-span | summary | uni-vlan [type]]
```

Syntax Description	
<b>access-map</b>	See the <a href="#">show vlan access-map</a> command.
<b>brief</b>	(Optional) Display one line for each VLAN with the VLAN name, status, and its ports.
<b>dot1q tag native</b>	(Optional) Display the IEEE 802.1Q native VLAN tagging status. This keyword is supported only when the switch is running the metro IP access or metro access image.
<b>filter</b>	See the <a href="#">show vlan filter</a> command.
<b>id <i>vlan-id</i></b>	(Optional) Display information about a single VLAN identified by VLAN ID number. For <i>vlan-id</i> , the range is 1 to 4094.
<b>internal usage</b>	(Optional) Display a list of VLANs being used internally by the switch. These VLANs are always from the extended range (VLAN IDs 1006 to 4094). You cannot create VLANs with these IDs by using the <b>vlan</b> global configuration command until you remove them from internal use. This keyword is supported only when the switch is running the metro IP access image.
<b>mtu</b>	(Optional) Display a list of VLANs and the minimum and maximum transmission unit (MTU) sizes configured on ports in the VLAN.
<b>name <i>vlan-name</i></b>	(Optional) Display information about a single VLAN identified by VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.
<b>private-vlan [<i>type</i>]</b>	(Optional) Display information about configured private VLANs, including primary and secondary VLAN IDs, type (community, isolated, or primary) and ports belonging to the private VLAN. Enter <b>type</b> (optional) to see only the VLAN ID and the type of private VLAN.
<b>remote-span</b>	(Optional) Display information about Remote SPAN (RSPAN) VLANs.
<b>summary</b>	(Optional) Display VLAN summary information.
<b>uni-vlan [<i>type</i>]</b>	(Optional) Display user network interface-enhanced network interface (UNI-ENI) VLAN information. Enter <b>type</b> (optional) to see only the VLAN ID and type of UNI-ENI VLAN.



### Note

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

### Command Modes

User EXEC

**Command History**

Release	Modification
12.2(44)EY	This command was introduced.

**Usage Guidelines**

In the **show vlan mtu** command output, the `MTU_Mismatch` column shows whether all the ports in the VLAN have the same MTU. When *yes* appears in this column, it means that the VLAN has ports with different MTUs. 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 a switch virtual interface (SVI), the hyphen (-) symbol appears in the `SVI_MTU` column. If the `MTU-Mismatch` column displays *yes*, the names of the port with the `MinMTU` and the port with the `MaxMTU` appear.

If you try to associate a private VLAN secondary VLAN with a primary VLAN before you define the secondary VLAN, the secondary VLAN is not included in the **show vlan private-vlan** command output.

In the **show vlan private-vlan type** command output, a *normal* type means a VLAN has a private VLAN association but is not part of the private VLAN. For example, if you define and associate two VLANs as primary and secondary VLANs and then delete the secondary VLAN configuration but do not remove the association from the primary VLAN, the VLAN that was the secondary VLAN is shown as *normal* in the display. In the **show vlan private-vlan** output, the primary and secondary VLAN pair is shown as *non-operational*.

In the **show vlan uni-vlan type** command output, type is either *community* or *isolated*. User network interfaces (UNIs) or enhanced network interfaced (ENIs) in a UNI-ENI community VLAN can communicate with each other; UNIs or ENIs in a UNI-ENI isolated VLAN cannot communicate. Network node interfaces (NNIs) can communicate with each other and with UNIs or ENIs in UNI-ENI isolated and community VLANs.

**Examples**

This is an example of output from the **show vlan** command. [Table 2-21](#) describes the fields in the display.

**Note**

The switch supports only Ethernet VLANs. You can configure parameters for FDDI and Token Ring VLANs and view the results in the `vlan.dat` file, but these parameters are not supported or used.

```
Switch> show vlan
Switch#show vlan
VLAN Name                Status    Ports
-----
1    default                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                         Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                         Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                         Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                         Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                         Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                         Gi0/1, Gi0/2

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
1002 fddi     101002    1500   -       -        -      -         0        0
1003 tr      101003    1500   -       -        -      -         0        0
1004 fdnet   101004    1500   -       -        -      ieee      0        0
1005 trnet   101005    1500   -       -        -      ibm       0        0
                                         0VLAN Name
```

```

Remote SPAN VLANs
-----
Primary Secondary Type          Ports
-----
VLAN Type          Ports
-----

```

**Table 2-21** *show vlan Command Output Fields*

Field	Description
VLAN	VLAN number.
Name	Name, if configured, of the VLAN.
Status	Status of the VLAN (active or suspend).
Ports	Ports that belong to the VLAN.
Type	Media type of the VLAN.
SAID	Security association ID value for the VLAN.
MTU	Maximum transmission unit size for the VLAN.
Parent	Parent VLAN, if one exists.
RingNo	Ring number for the VLAN, if applicable.
BrdgNo	Bridge number for the VLAN, if applicable.
Stp	Spanning Tree Protocol type used on the VLAN.
BrdgMode	Bridging mode for this VLAN—possible values are source-route bridging (SRB) and source-route transparent (SRT); the default is SRB.
Trans1	Translation bridge 1.
Trans2	Translation bridge 2.
Remote SPAN VLANs	Identifies any RSPAN VLANs that have been configured.
Primary/Secondary/ Type/Ports	Includes any configured private VLANs, including the primary VLAN ID, the secondary VLAN ID, the type of secondary VLAN (community or isolated), and the ports that belong to it.
VLAN Type/Ports	Displays any configured UNI-ENI VLANs, the type (community or isolated), and the ports that belong to it.

This is an example of output from the **show vlan dot1q tag native** command:

```

Switch> show vlan dot1q tag native
dot1q native vlan tagging is disabled

```



This is an example of output from the **show vlan private-vlan** command:

```
Switch> show vlan private-vlan
Primary Secondary Type Ports
-----
10 501 isolated Gi0/3
10 502 community Fa0/11
10 503 non-operational3 -
20 25 isolated Fa0/13, Fa0/20, Fa0/22, Gi0/1,
20 30 community Fa0/13, Fa0/20, Fa0/21, Gi0/1,
20 35 community Fa0/13, Fa0/20, Fa0/23, Fa0/33. Gi0/1,
20 55 non-operational
2000 2500 isolated Fa0/5, Fa0/10, Fa0/15
```

This is an example of output from the **show vlan private-vlan type** command:

```
Switch> show vlan private-vlan type
Vlan Type
-----
10 primary
501 isolated
502 community
503 normal
```

This is an example of output from the **show vlan uni-vlan type** command:

```
Switch> show vlan uni-vlan type
Vlan Type
-----
1 UNI isolated
20 UNI community
201 UNI isolated
```

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

```
Switch> show vlan summary
Number of existing VLANs : 45
Number of existing VTP VLANs : 0
Number of existing extended VLANs : 0
```

This is an example of output from the **show vlan id** command.

```
Switch# show vlan id 2
VLAN Name Status Ports
-----
2 VLAN0200 active Gi0/1, Gi0/2

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
-----
2 enet 100002 1500 - - - - - 0 0

Remote SPAN VLAN
-----
Disabled
```

This is an example of output from the **show vlan internal usage** command. It shows that VLANs 1025 and 1026 are being used as internal VLANs for Fast Ethernet routed ports 23 and 24. If you want to use one of these VLAN IDs, you must first shut down the routed port, which releases the internal VLAN, and then create the extended-range VLAN. When you start up the routed port, another internal VLAN number is assigned to it.

```
Switch> show vlan internal usage
VLAN Usage
-----
1025 FastEthernet0/23
1026 FastEthernet0/24
```

#### Related Commands

Command	Description
<a href="#">private-vlan</a>	Configures a VLAN as a community, isolated, or primary VLAN or associates a primary VLAN with secondary VLANs.
<a href="#">switchport mode</a>	Configures the VLAN membership mode of a port.
<a href="#">vlan</a>	Enables VLAN configuration mode where you can configure VLANs 1 to 4094.

# show vlan access-map

Use the **show vlan access-map** privileged EXEC command to display information about a particular VLAN access map or for all VLAN access maps.

**show vlan access-map** [*mapname*]

<b>Syntax Description</b>	<i>mapname</i> (Optional) Name of a specific VLAN access map.
---------------------------	---

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

**Examples** This is an example of output from the **show vlan access-map** command:

```
Switch# show vlan access-map
Vlan access-map "SecWiz" 10
  Match clauses:
    ip address: SecWiz_Fa1_0_3_in_ip
  Action:
    forward
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show vlan filter</a>	Displays information about all VLAN filters or about a particular VLAN or VLAN access map.
	<a href="#">vlan access-map</a>	Creates a VLAN map entry for VLAN packet filtering.
	<a href="#">vlan filter</a>	Applies a VLAN map to one or more VLANs.

# show vlan filter

Use the **show vlan filter** privileged EXEC command to display information about all VLAN filters or about a particular VLAN or VLAN access map.

```
show vlan filter [access-map name | vlan vlan-id]
```

Syntax Description	access-map name	(Optional) Display filtering information for the specified VLAN access map.
	vlan vlan-id	(Optional) Display filtering information for the specified VLAN. The range is 1 to 4094.

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

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Examples** This is an example of output from the **show vlan filter** command:

```
Switch# show vlan filter
VLAN Map map_1 is filtering VLANs:
 20-22
```

Related Commands	Command	Description
	<a href="#">show vlan access-map</a>	Displays information about a particular VLAN access map or for all VLAN access maps.
	<a href="#">vlan access-map</a>	Creates a VLAN map entry for VLAN packet filtering.
	<a href="#">vlan filter</a>	Applies a VLAN map to one or more VLANs.

# show vlan mapping

Use the **show vlan mapping** privileged EXEC command to display information about VLAN mapping on trunk ports.

**show vlan mapping** [*interface interface-id* | *usage*]

Syntax Description		
<b>interface</b> <i>interface-id</i>	(Optional) Display VLAN mapping information for the specified interface.	
<b>usage</b>	(Optional) Display hardware resources used in VLAN mapping.	

**Defaults** There is no default.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Examples** This is an example of output from the **show vlan mapping** command:

```
Switch# show vlan mapping
Interface Fa0/5:
VLANs on wire      Translated VLAN      Operation
-----
default QinQ      1                    selective QinQ
Interface Fa0/2:
VLANs on wire      Translated VLAN      Operation
-----
2                  104                  1-to-1 mapping
```

This is an example of output from the **show vlan mapping** command for an interface:

```
Switch# show vlan mapping interface fa0/6
Interface fa0/6:
VLAN on wire      Translated VLAN      Operation
1                  11                   1-to-1 mapping
12,16-18          100                  selective QinQ
*                  101                  default QinQ
```

## show vlan mapping

These are examples of output from the **show vlan mapping usage** command:

```
Switch# show vlan mapping usage
Ports:Gi0/1-Gi0/2,Fa0/1-Fa0/24
Vlan Mapping resource usage is 1%
```

```
Switch# show vlan mapping usage
Ports:Gi0/1-Gi0/4
Vlan Mapping resource usage is 0%
```

```
Ports:Gi0/5-Gi0/8
Vlan Mapping resource usage is 0%
```

```
Ports:Gi0/9-Gi0/12
Vlan Mapping resource usage is 0%
```

```
Ports:Gi0/13-Gi0/16
Vlan Mapping resource usage is 0%
```

### Related Commands

Command	Description
<a href="#">switchport vlan mapping</a>	Configures VLAN mapping on an interface.

# show vmps

Use the **show vmps** user EXEC command without keywords 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, or use the **statistics** keyword to display client-side statistics.

**show vmps [statistics]**

<b>Syntax Description</b>	<b>statistics</b> (Optional) Display VQP client-side statistics and counters.				
<b>Command Modes</b>	User EXEC				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(44)EY</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(44)EY	This command was introduced.
Release	Modification				
12.2(44)EY	This command was introduced.				

## Examples

This is an example of output from the **show vmps statistics** command.

```
Switch> 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 2-22 describes each field in the display.

**Table 2-22** *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 re-enable 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.

■ show vmps

**Table 2-22** *show vmps statistics Field Descriptions (continued)*

Field	Description
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 VQP 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 Commands	Command	Description
	<a href="#">clear vmps statistics</a>	Clears the statistics maintained by the VQP client.
	<a href="#">vmps reconfirm (privileged EXEC)</a>	Sends VQP queries to reconfirm all dynamic VLAN assignments with the VMPS.
	<a href="#">vmps retry</a>	Configures the per-server retry count for the VQP client.
	<a href="#">vmps server</a>	Configures the primary VMPS and up to three secondary servers.



# shutdown

Use the **shutdown** interface configuration command to disable an interface. Use the **no** form of this command to restart a disabled interface.

**shutdown**

**no shutdown**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The **shutdown** command causes a port to stop forwarding. The default state for a user network interface (UNI) or enhanced network interface (ENI) is shut down. Before you can configure a UNI or ENI, you must enable it with the **no shutdown** command. Network node interfaces (NNIs) are enabled by default.

The **no shutdown** command has no effect if the port is a static-access port assigned to a VLAN that has been deleted, suspended, or shut down. The port must first be a member of an active VLAN before it can be re-enabled.

The **shutdown** command disables all functions on the specified interface.

This command also marks the interface as unavailable. To see if an interface is disabled, use the **show interfaces** privileged EXEC command. An interface that has been shut down is shown as administratively down in the display.

## Examples

These examples show how to disable and re-enable a port:

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

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no shutdown
```

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

## Related Commands

Command	Description
<a href="#">show interfaces</a>	Displays the statistical information specific to all interfaces or to a specific interface.

# shutdown vlan

Use the **shutdown vlan** global configuration command to shut down (suspend) local traffic on the specified VLAN. Use the **no** form of this command to restart local traffic on the VLAN.

**shutdown vlan** *vlan-id*

**no shutdown vlan** *vlan-id*

<b>Syntax Description</b>	<i>vlan-id</i>	ID of the VLAN to be locally shut down. The range is 2 to 1001. VLANs defined as default VLANs (1 and 1002 to 1005), as well as extended-range VLANs (greater than 1005) cannot be shut down.
<b>Defaults</b>	No default is defined.	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.
<b>Usage Guidelines</b>	Use the shutdown VLAN configuration command to shut down local traffic on any VLAN, including extended-range VLANs (1006-4094).	
<b>Examples</b>	<p>This example shows how to shut down traffic on VLAN 2:</p> <pre>Switch(config)# <b>shutdown vlan 2</b></pre> <p>You can verify your setting by entering the <b>show vlan</b> privileged EXEC command.</p>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>shutdown</b> (VLAN configuration)	Shuts down local traffic on the VLAN when in VLAN configuration mode (accessed by the <b>vlan</b> <i>vlan-id</i> global configuration command).

## snmp mib rep trap-rate

Use the **snmp mib rep trap-rate** global configuration command to configure the sending of Resilient Ethernet Protocol (REP) SNMP traps when there is a link operational status or port role change. Use the **no** version of the command to disable sending of the REP trap.

**snmp mib rep trap-rate** *value*

**no snmp mib rep trap-rate**

<b>Syntax Description</b>	<b>trap-rate</b> <i>value</i> Set the number of REP 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).
---------------------------	--

<b>Defaults</b>	Sending REP traps is disabled.
-----------------	--------------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

<b>Usage Guidelines</b>	Use this command to enable the switch to send REP specific traps corresponding to link operational status changes and port role changes.
-------------------------	--

<b>Examples</b>	This example configures the switch to send REP traps at a rate of 10 per second:
-----------------	--

```
Switch(config)# snmp mib rep trap-rate 10
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show running config</b>	Verifies that REP traps are configured.

## snmp-server enable traps

Use the **snmp-server enable traps** global configuration command to enable the switch to send Simple Network Management Protocol (SNMP) notifications for various traps or inform requests to the network management system (NMS). Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps [bgp | bridge [newroot] [topologychange] | config | copy-config | cpu
threshold | {dot1x [auth-fail-vlan | guest-vlan | no-auth-fail-vlan | no-guest-vlan]} | entity
| envmon [fan | shutdown | status | supply | temperature] | ethernet | flash | hsrp | ipmulticast
| mac-notification [change] [move] [threshold] | msdp | ospf [cisco-specific | errors | lsa |
rate-limit | retransmit | state-change] | pim [invalid-pim-message | neighbor-change |
rp-mapping-change] | port-security [trap-rate value] | rtr | snmp [authentication | coldstart
| linkdown | linkup | warmstart] | storm-control trap-rate value | stpx [inconsistency]
| root-inconsistency] | loop-inconsistency] | syslog | transceiver all | tty | vlan-membership |
vlancreate | vlandelete]
```

```
no snmp-server enable traps [bgp | bridge [newroot] [topologychange] | config | copy-config |
cpu threshold | {dot1x [auth-fail-vlan | guest-vlan | no-auth-fail-vlan | no-guest-vlan]} |
entity | envmon [fan | shutdown | status | supply | temperature] | ethernet | flash | hsrp |
ipmulticast | mac-notification [change] [move] [threshold] | msdp | ospf [cisco-specific |
errors | lsa | rate-limit | retransmit | state-change] | pim [invalid-pim-message |
neighbor-change | rp-mapping-change] | port-security [trap-rate value] | rtr | snmp
[authentication | coldstart | linkdown | linkup | warmstart] | storm-control trap-rate value
| stpx [inconsistency] | root-inconsistency] | loop-inconsistency] | syslog | transceiver all |
tty | vlan-membership | vlancreate | vlandelete]
```

### Syntax Description

<b>bgp</b>	(Optional) Enable Border Gateway Protocol (BGP) state-change traps. <b>Note</b> This keyword is supported only when the metro IP access image is running on the switch.
<b>bridge [newroot] [topologychange]</b>	(Optional) Generate Spanning Tree Protocol (STP) bridge MIB traps. The keywords have these meanings: <ul style="list-style-type: none"> <li><b>newroot</b>—(Optional) Enable SNMP STP bridge MIB new root traps.</li> <li><b>topologychange</b>—(Optional) Enable SNMP STP bridge MIB topology change traps.</li> </ul>
<b>config</b>	(Optional) Enable SNMP configuration traps.
<b>copy-config</b>	(Optional) Enable SNMP copy-configuration traps.
<b>cpu threshold</b>	(Optional) Allow CPU-related traps.

<b>dot1x</b> [ <b>auth-fail-vlan</b>   <b>guest-vlan</b>   <b>no-auth-fail-vlan</b>   <b>no-guest-vlan</b> ]	(Optional) Enable IEEE 802.1x traps. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>auth-fail-vlan</b>—(Optional) Generate a trap when the port moves to the configured restricted VLAN.</li> <li>• <b>guest-vlan</b>—(Optional) Generate a trap when the port moves to the configured guest VLAN.</li> <li>• <b>no-auth-fail-vlan</b>—(Optional) Generate a trap when a port tries to enter the restricted VLAN, but cannot because the restricted VLAN is not configured.</li> <li>• <b>no-guest-vlan</b>—(Optional) Generate a trap when a port tries to enter the guest VLAN, but cannot because the guest VLAN is not configured.</li> </ul> <p><b>Note</b> When the <b>snmp-server enable traps dot1x</b> command is entered (without any other keywords specified), all the IEEE 802.1x traps are enabled.</p>
<b>entity</b>	(Optional) Enable SNMP entity traps.
<b>envmon</b> [ <b>fan</b>   <b>shutdown</b>   <b>status</b>   <b>supply</b>   <b>temperature</b> ]	(Optional) Enable SNMP environmental traps. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>fan</b>—(Optional) Enable fan traps.</li> <li>• <b>shutdown</b>—(Optional) Enable environmental monitor shutdown traps.</li> <li>• <b>status</b>—(Optional) Enable SNMP environmental status-change traps.</li> <li>• <b>supply</b>—(Optional) Enable environmental monitor power-supply traps.</li> <li>• <b>temperature</b>—(Optional) Enable environmental monitor temperature traps.</li> </ul>
<b>ethernet</b>	(Optional) Enable SNMP Ethernet traps.
<b>flash</b>	(Optional) Enable SNMP flash notifications.
<b>hsrp</b>	(Optional) Enable Hot Standby Router Protocol (HSRP) traps.
<b>ipmulticast</b>	(Optional) Enable IP multicast routing traps.
<b>mac-notification</b>	(Optional) Enable MAC address notification traps.
<b>change</b>	(Optional) Enable MAC address change notification traps.
<b>move</b>	(Optional) Enable MAC address move notification traps.
<b>threshold</b>	(Optional) Enable MAC address table threshold traps.
<b>msdp</b>	(Optional) Enable Multicast Source Discovery Protocol (MSDP) traps.
<b>ospf</b> [ <b>cisco-specific</b>   <b>errors</b>   <b>lsa</b>   <b>rate-limit</b>   <b>retransmit</b>   <b>state-change</b> ]	(Optional) Enable Open Shortest Path First (OSPF) traps. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>cisco-specific</b>—(Optional) Enable Cisco-specific traps.</li> <li>• <b>errors</b>—(Optional) Enable error traps.</li> <li>• <b>lsa</b>—(Optional) Enable link-state advertisement (LSA) traps.</li> <li>• <b>rate-limit</b>—(Optional) Enable rate-limit traps.</li> <li>• <b>retransmit</b>—(Optional) Enable packet-retransmit traps.</li> <li>• <b>state-change</b>—(Optional) Enable state-change traps.</li> </ul>

<b>pim</b> [invalid-pim-message   neighbor-change   rp-mapping-change]	(Optional) Enable Protocol-Independent Multicast (PIM) traps. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>invalid-pim-message</b>—(Optional) Enable invalid PIM message traps.</li> <li>• <b>neighbor-change</b>—(Optional) Enable PIM neighbor-change traps.</li> <li>• <b>rp-mapping-change</b>—(Optional) Enable rendezvous point (RP)-mapping change traps.</li> </ul>
<b>port-security</b> [trap-rate <i>value</i> ]	(Optional) Enable port security traps. Use the <b>trap-rate</b> keyword to set 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 port-security occurrence).
<b>rtr</b>	(Optional) Enable SNMP Response Time Reporter traps.
<b>snmp</b> [authentication   coldstart   linkdown   linkup   warmstart]	(Optional) Enable SNMP traps. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>authentication</b>—(Optional) Enable authentication trap.</li> <li>• <b>coldstart</b>—(Optional) Enable cold-start trap.</li> <li>• <b>linkdown</b>—(Optional) Enable linkdown trap.</li> <li>• <b>linkup</b>—(Optional) Enable linkup trap.</li> <li>• <b>warmstart</b>—(Optional) Enable warm-start trap.</li> </ul>
<b>storm-control</b> trap-rate <i>value</i>	(Optional) Enable storm-control traps. Use the <b>trap-rate</b> keyword to set the maximum number of storm-control traps sent per minute. The range is from 0 to 1000; the default is 0 (no limit is imposed; a trap is sent at every storm-control occurrence).
<b>stpx</b> [inconsistency] [root-inconsistency] [loop-inconsistency]	(Optional) Enable SNMP STPX MIB traps. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>inconsistency</b>—(Optional) Enable SNMP STPX MIB inconsistency update traps.</li> <li>• <b>root-inconsistency</b>—(Optional) Enable SNMP STPX MIB root inconsistency update traps.</li> <li>• <b>loop-inconsistency</b>—(Optional) Enable SNMP STPX MIB loop inconsistency update traps.</li> </ul>
<b>syslog</b>	(Optional) Enable SNMP syslog traps.
<b>transceiver all</b>	(Optional) Enable SNMP traps for all supported Digital Optical Monitoring (DoM)-capable transceivers installed on the switch.
<b>tty</b>	(Optional) Send TCP connection traps. This is enabled by default.
<b>vlan-membership</b>	(Optional) Enable SNMP VLAN membership traps.
<b>vlancreate</b>	(Optional) Enable SNMP VLAN-created traps.
<b>vlandelete</b>	(Optional) Enable SNMP VLAN-deleted traps.

**Note**

Though visible in the command-line help strings, the **fru-ctrl insertion** and **removal**, and **vtp** keywords are not supported. The **snmp-server enable informs** global configuration command is not supported. To enable the sending of SNMP inform notifications, use the **snmp-server enable traps** global configuration command combined with the **snmp-server host *host-addr* informs** global configuration command.

**Defaults** The sending of SNMP traps is disabled.

**Command Modes** Global configuration

Release	Modification
12.2(44)EY	This command was introduced.
12.2(50)SE	The <b>cpu threshold</b> keywords were added.
12.2(52)SE	The <b>transceiver all</b> keywords were added.

**Usage Guidelines** Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

When supported, use the **snmp-server enable traps** command to enable sending of traps or informs.



**Note** Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

SNMP transceiver traps apply to SFPs that support DoM-capable transceivers installed on the switch. The sensor values are polled every 10 minutes, which is how often the user sees traps or alarms.

**Examples** This example shows how to send port security traps to the NMS:

```
Switch(config)# snmp-server enable traps port security
```

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

Command	Description
<b>show running-config</b>	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: <a href="http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html">http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html</a> Select the <b>Cisco IOS Commands Master List, Release 12.2</b> to navigate to the command.
<b>snmp-server host</b>	Specifies the host that receives SNMP traps.

## snmp-server host

Use the **snmp-server host** global configuration command to specify the recipient (host) of a Simple Network Management Protocol (SNMP) notification operation. Use the **no** form of this command to remove the specified host.

```
snmp-server host host-addr [informs | traps] [version {1 | 2c | 3 {auth | noauth | priv}}] [vrf
vrf-instance] [community-string [notification-type]]
```

```
no snmp-server host host-addr [informs | traps] [version {1 | 2c | 3 {auth | noauth | priv}}] [vrf
vrf-instance] community-string
```

### Syntax Description

<i>host-addr</i>	Name or Internet address of the host (the targeted recipient).
<b>udp-port</b> <i>port</i>	(Optional) Configure the User Datagram Protocol (UDP) port number of the host to receive the traps. The range is from 0 to 65535.
<b>informs</b>   <b>traps</b>	(Optional) Send SNMP traps or informs to this host.
<b>version</b> <b>1</b>   <b>2c</b>   <b>3</b>	(Optional) Version of the SNMP used to send the traps. These keywords are supported: <b>1</b> —SNMPv1. This option is not available with informs. <b>2c</b> —SNMPv2C. <b>3</b> —SNMPv3. These optional keywords can follow the Version 3 keyword: <ul style="list-style-type: none"> <li><b>auth</b> (Optional). Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication.</li> <li><b>noauth</b> (Default). The noAuthNoPriv security level. This is the default if the [<b>auth</b>   <b>noauth</b>   <b>priv</b>] keyword choice is not specified.</li> <li><b>priv</b> (Optional). Enables Data Encryption Standard (DES) packet encryption (also called <i>privacy</i>).</li> </ul> <b>Note</b> The <b>priv</b> keyword is available only when the cryptographic (encrypted) software image is installed.
<b>vrf</b> <i>vrf-instance</i>	(Optional) Virtual private network (VPN) routing instance and name for this host.
<i>community-string</i>	Password-like community string sent with the notification operation. Though you can set this string by using the <b>snmp-server host</b> command, we recommend that you define this string by using the <b>snmp-server community</b> global configuration command before using the <b>snmp-server host</b> command. <b>Note</b> The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.



*notification-type*

(Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent. The notification type can be one or more of the these keywords:

- Note** The **bgp**, **hsrp**, **ipmulticast**, **mdsp**, **ospf**, and **pim** keywords are available only when the metro IP access image is installed on the switch.
- **bgp**—Send Border Gateway Protocol (BGP) state change traps. This keyword is valid only when the metro IP access image is installed on the switch.
  - **bridge**—Send SNMP Spanning Tree Protocol (STP) bridge MIB traps.
  - **config**—Send SNMP configuration traps.
  - **copy-config**—Send SNMP copy configuration traps.
  - **cpu threshold**—Allow CPU-related traps.
  - **entity**— Send SNMP entity traps.
  - **envmon**—Send environmental monitor traps.
  - **flash**—Send SNMP FLASH notifications.
  - **hsrp**—Send SNMP Hot Standby Router Protocol (HSRP) traps.
  - **ipmulticast**—Send SNMP IP multicast routing traps.
  - **mac-notification**—Send SNMP MAC notification traps.
  - **msdp**—Send SNMP Multicast Source Discovery Protocol (MSDP) traps.
  - **ospf**—Send Open Shortest Path First (OSPF) traps.
  - **pim**—Send SNMP Protocol-Independent Multicast (PIM) traps.
  - **port-security**—Send SNMP port-security traps.
  - **rtr**—Send SNMP Response Time Reporter traps.
  - **snmp**—Send SNMP-type traps.
  - **storm-control**—Send SNMP storm-control traps.
  - **stp**—Send SNMP STP extended MIB traps.
  - **syslog**—Send SNMP syslog traps.
  - **tty**—Send TCP connection traps.
  - **vlan-membership**— Send SNMP VLAN membership traps.
  - **vlancreate**—Send SNMP VLAN-created traps.
  - **vlandelete**—Send SNMP VLAN-deleted traps.

**Note**

Though visible in the command-line help strings, the **fru-ctrl**, and **vtp** keywords are not supported.

**Defaults**

This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs are sent to this host.

If no **version** keyword is present, the default is Version 1.

If Version 3 is selected and no authentication keyword is entered, the default is the **noauth** (noAuthNoPriv) security level.

**Command Modes**

Global configuration

**Command History**

Release	Modification
12.2(44)EY	This command was introduced.
12.2(50)SE	The <b>cpu threshold</b> keywords were added.

**Usage Guidelines**

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destinations.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Traps are also sent only once, but an inform might be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the switch to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host. To enable multiple hosts, you must enter a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

If a local user is not associated with a remote host, the switch does not send informs for the **auth** (authNoPriv) and the **priv** (authPriv) authentication levels.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command is in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command replaces the first.

The **snmp-server host** command is used with the **snmp-server enable traps** global configuration command. Use the **snmp-server enable traps** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled. Some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled. Other notification types are enabled by a different command.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.

---

**Examples**

This example shows how to configure a unique SNMP community string named *comaccess* for traps and prevent SNMP polling access with this string through access-list 10:

```
Switch(config)# snmp-server community comaccess ro 10
Switch(config)# snmp-server host 172.20.2.160 comaccess
Switch(config)# access-list 10 deny any
```

This example shows how to send the SNMP traps to the host specified by the name *myhost.cisco.com*. The community string is defined as *comaccess*:

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com comaccess snmp
```

This example shows how to enable the switch to send all traps to the host *myhost.cisco.com* by using the community string *public*:

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

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

---

**Related Commands**

Command	Description
<b>show running-config</b>	Displays the operating configuration.
<b>snmp-server enable traps</b>	Enables SNMP notification for various trap types or inform requests.

## snmp trap mac-notification change

Use the **snmp trap mac-notification change** interface configuration command to enable the Simple Network Management Protocol (SNMP) MAC address notification trap on a specific Layer 2 interface. Use the **no** form of this command to return to the default setting.

**snmp trap mac-notification change {added | removed}**

**no snmp trap mac-notification change {added | removed}**

### Syntax Description

<b>added</b>	Enable the MAC notification trap whenever a MAC address is added on this interface.
<b>removed</b>	Enable the MAC notification trap whenever a MAC address is removed from this interface.

### Defaults

By default, the traps for both address addition and address removal are disabled.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

Even though you enable the notification trap for a specific interface by using the **snmp trap mac-notification** command, the trap is generated only when you enable the **snmp-server enable traps mac-notification** and the **mac address-table notification** global configuration commands.

### Examples

This example shows how to enable the MAC notification trap when a MAC address is added to a port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# snmp trap mac-notification change added
```

You can verify your settings by entering the **show mac address-table notification change interface** privileged EXEC command.

Related Commands	Command	Description
	<b>clear mac address-table notification</b>	Clears the MAC address notification global counters.
	<b>mac address-table notification</b>	Enables the MAC address notification feature.
	<b>show mac address-table notification</b>	Displays the MAC address notification settings for all interfaces or on the specified interface when the <b>interface</b> keyword is appended.
	<b>snmp-server enable traps</b>	Sends the SNMP MAC notification traps when the <b>mac-notification</b> keyword is appended.

# spanning-tree

Use the **spanning-tree** interface configuration command with no keywords on an enhanced network interface (ENI) to enable a spanning-tree instance on the interface. Use the **no** form of this command to return to the default setting of disabled.

**spanning-tree**

**no spanning-tree**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The Spanning-Tree Protocol (STP) is disabled on ENIs.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

This command is supported only on ENIs and on EtherChannel port channels that contain ENIs.

STP is not supported on user network interfaces (UNIs) and it is disabled by default on ENIs. Use this command to enable SPT on an ENI. To set a port as an ENI, enter the **port-type eni** interface configuration command. Once STP is enabled on an ENI, all other STP interface configuration commands are available on the interface.

The switch supports only one spanning-tree instance on a VLAN. When NNIs and ENIs with spanning tree enabled are in the same VLAN, they belong to the same spanning-tree instance.

STP is enabled by default on NNIs. UNIs are typically customer-facing ports and do not participate in the spanning tree of the service provider. However, if you configure a customer-facing port as an ENI and enable spanning tree, the ENI could become the spanning tree root port unless you configure root guard on the port by using the **spanning-tree guard root** interface configuration command. A customer-facing ENI with STP enabled participates in the same spanning tree as the service-provider facing NNI.



### Note

Exercise caution when enabling STP on a customer-facing ENI.

## Examples

This example shows how to enable STP on a port:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# port-type eni
Switch(config-if)# spanning-tree
```

You can verify your setting by entering the **show spanning-tree interface** privileged EXEC command.

Related Commands	Command	Description
	<b>show spanning-tree interface</b> <i>interface-id</i>	Display spanning-tree information for the specified interface.

## spanning-tree bpdudfilter

Use the **spanning-tree bpdudfilter** interface configuration command on a network node interface (NNI) or enhanced network interface (ENI) with STP enabled to prevent the interface from sending or receiving bridge protocol data units (BPDUs). Use the **no** form of this command to return to the default setting.

**spanning-tree bpdudfilter** { **disable** | **enable** }

**no spanning-tree bpdudfilter**

Syntax Description	disable	Disable BPDU filtering on the specified STP port.
	enable	Enable BPDU filtering on the specified STP port.

**Defaults** BPDU filtering is disabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). You can configure BPDU filtering only on NNIs or on ENIs on which STP has been enabled. To set a port as an NNI or ENI, enter the **port-type** { **nni** | **eni** } interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

You can enable the BPDU filtering feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode.



### Caution

Enabling BPDU filtering on an STP port is the same as disabling spanning tree on it and can result in spanning-tree loops.

You can globally enable BPDU filtering on all Port Fast-enabled STP ports by using the **spanning-tree portfast bpdudfilter default** global configuration command.

You can use the **spanning-tree bpdudfilter** interface configuration command on an STP port to override the setting of the **spanning-tree portfast bpdudfilter default** global configuration command.

**Examples** This example shows how to enable the BPDU filtering feature on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree bpdudfilter enable
```

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



Related Commands	Command	Description
	<b>show running-config</b>	Displays the operating configuration.
	<b>spanning-tree portfast (global configuration)</b>	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled STP ports or enables the Port Fast feature on all nontrunking STP ports.
	<b>spanning-tree portfast (interface configuration)</b>	Enables the Port Fast feature on an STP port and all its associated VLANs.

# spanning-tree bpduguard

Use the **spanning-tree bpduguard** interface configuration command on a network node interface (NNI) or enhanced network interface (ENI) with STP enabled to put the interface in the error-disabled state when it receives a bridge protocol data unit (BPDU). Use the **no** form of this command to return to the default setting.

**spanning-tree bpduguard { disable | enable }**

**no spanning-tree bpduguard**

Syntax Description	disable	Disable BPDU guard on the specified STP port.
	enable	Enable BPDU guard on the specified STP port.

**Defaults** BPDU guard is disabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). You can configure BPDU guard only on NNIs or on ENIs on which STP has been enabled. To set a port as an NNI or ENI, enter the **port-type { nni | eni }** interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

The BPDU guard feature provides a secure response to invalid configurations because you must manually put the STP port back in service. Use the BPDU guard feature in a service-provider network to prevent an interface from being included in the spanning-tree topology.

You can enable the BPDU guard feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), the rapid-PVST+, or the multiple spanning-tree (MST) mode.

You can globally enable BPDU guard on all Port Fast-enabled STP ports by using the **spanning-tree portfast bpduguard default** global configuration command.

You can use the **spanning-tree bpduguard** interface configuration command on an STP port to override the setting of the **spanning-tree portfast bpduguard default** global configuration command.

**Examples** This example shows how to enable the BPDU guard feature on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree bpduguard enable
```

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

Related Commands	Command	Description
	<b>show running-config</b>	Displays the operating configuration.
	<b>spanning-tree portfast (global configuration)</b>	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled STP ports or enables the Port Fast feature on all nontrunking STP ports.
	<b>spanning-tree portfast (interface configuration)</b>	Enables the Port Fast feature on an STP port and all its associated VLANs.

## spanning-tree cost

Use the **spanning-tree cost** interface configuration command on a network node interface (NNI) or enhanced network interface (ENI) with STP enabled to set the path cost for spanning-tree calculations. If a loop occurs, spanning tree considers the path cost when selecting an interface to place in the forwarding state. Use the **no** form of this command to return to the default setting.

**spanning-tree** [vlan *vlan-id*] **cost** *cost*

**no spanning-tree** [vlan *vlan-id*] **cost**

### Syntax Description

<b>vlan</b> <i>vlan-id</i>	(Optional) VLAN range associated with a spanning-tree instance. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
<i>cost</i>	Path cost. The range is 1 to 200000000, with higher values meaning higher costs.

### Defaults

The default path cost is computed from the STP port bandwidth setting. These are the IEEE default path cost values:

- 1000 Mbps—4
- 100 Mbps—19
- 10 Mbps—100

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). You can configure **spanning-tree cost** only on NNIs or on enhanced network interfaces (ENIs) on which STP has been enabled. To set a port as an NNI or ENI, enter the **port-type {nni | eni}** interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

When you configure the cost, higher values represent higher costs.

If you configure an STP port with both the **spanning-tree vlan *vlan-id* cost *cost*** command and the **spanning-tree cost *cost*** command, the **spanning-tree vlan *vlan-id* cost *cost*** command takes effect.

### Examples

This example shows how to set the path cost to 250 on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree cost 250
```

This example shows how to set a path cost to 300 for VLANs 10, 12 to 15, and 20:

```
Switch(config-if)# spanning-tree vlan 10,12-15,20 cost 300
```

You can verify your settings by entering the **show spanning-tree interface *interface-id*** privileged EXEC command.

Related Commands	Command	Description
	<b>show spanning-tree interface <i>interface-id</i></b>	Displays spanning-tree information for the specified interface.
	<b>spanning-tree port-priority</b>	Configures an STP port priority.
	<b>spanning-tree vlan priority</b>	Sets the switch priority for the specified spanning-tree instance.

## spanning-tree etherchannel guard misconfig

Use the **spanning-tree etherchannel guard misconfig** global configuration command to display an error message when the switch detects an EtherChannel misconfiguration. Use the **no** form of this command to disable the feature.

**spanning-tree etherchannel guard misconfig**

**no spanning-tree etherchannel guard misconfig**

### Syntax Description

This command has no arguments or keywords.

### Defaults

EtherChannel guard is enabled on the switch.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). This command affects only network node interfaces (NNIs) or enhanced network interfaces (ENIs) on which STP has been enabled. To set a port as an NNI or ENI, enter the **port-type {nni | eni}** interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

When the switch detects an EtherChannel misconfiguration, this error message appears:

```
PM-4-ERR_DISABLE: Channel-misconfig error detected on [chars], putting [chars] in
err-disable state.
```

To show switch ports that are in the misconfigured EtherChannel, use the **show interfaces status err-disabled** privileged EXEC command. To verify the EtherChannel configuration on a remote device, use the **show etherchannel summary** privileged EXEC command on the remote device.

When a port is in the error-disabled state because of an EtherChannel misconfiguration, you can bring it out of this state by entering the **errdisable recovery cause channel-misconfig** global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shut down** interface configuration commands.

### Examples

This example shows how to enable the EtherChannel guard misconfiguration feature:

```
Switch(config)# spanning-tree etherchannel guard misconfig
```

You can verify your settings by entering the **show spanning-tree summary** privileged EXEC command.

Related Commands	Command	Description
	<b>errdisable recovery cause channel-misconfig</b>	Enables the timer to recover from the EtherChannel misconfiguration error-disable state.
	<b>show etherchannel summary</b>	Displays EtherChannel information for a channel as a one-line summary per channel-group.
	<b>show interfaces status err-disabled</b>	Displays the interfaces in the error-disabled state.

# spanning-tree extend system-id

Use the **spanning-tree extend system-id** global configuration command to enable the extended system ID feature.

## spanning-tree extend system-id



### Note

Though visible in the command-line help strings, the **no** version of this command is not supported. You cannot disable the extended system ID feature.

### Syntax Description

This command has no arguments or keywords.

### Defaults

The extended system ID is enabled.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). This command affects only network node interfaces (NNIs) or enhanced network interfaces (ENIs) on which STP has been enabled. To set a port as an NNI or ENI, enter the **port-type { nni | eni }** interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

The switch supports the IEEE 802.1t spanning-tree extensions. Some of the bits previously used for the switch priority are now used for the extended system ID (VLAN identifier for the per-VLAN spanning-tree plus [PVST+] and rapid PVST+ or as an instance identifier for the multiple spanning tree [MST]).

The spanning tree uses the extended system ID, the switch priority, and the allocated spanning-tree MAC address to make the bridge ID unique for each VLAN or multiple spanning-tree instance.

Support for the extended system ID affects how you manually configure the root switch, the secondary root switch, and the switch priority of a VLAN. For more information, see the “[spanning-tree mst root](#)” and the “[spanning-tree vlan](#)” sections.

If your network consists of switches that do not support the extended system ID and switches that do support it, it is unlikely that the switch with the extended system ID support will become the root switch. The extended system ID increases the switch priority value every time the VLAN number is greater than the priority of the connected switches.



Related Commands	Command	Description
	<a href="#">show spanning-tree summary</a>	Displays a summary of spanning-tree interface states.
	<a href="#">spanning-tree mst root</a>	Configures the MST root switch priority and timers based on the network diameter.
	<a href="#">spanning-tree vlan priority</a>	Sets the switch priority for the specified spanning-tree instance.

## spanning-tree guard

Use the **spanning-tree guard** interface configuration command on a network node interface (NNI) or enhanced network interface (ENI) with STP enabled to enable root guard or loop guard on all the VLANs associated with the selected NNI. Root guard restricts which interface is allowed to be the spanning-tree root port or the path-to-the root for the switch. Loop guard prevents alternate or root ports from becoming designated ports when a failure creates a unidirectional link. Use the **no** form of this command to return to the default setting.

**spanning-tree guard** {loop | none | root}

**no spanning-tree guard**

### Syntax Description

<b>loop</b>	Enable loop guard.
<b>none</b>	Disable root guard or loop guard.
<b>root</b>	Enable root guard.

### Defaults

Root guard is disabled.

Loop guard is configured according to the **spanning-tree loopguard default** global configuration command (globally disabled).

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). You can configure spanning-tree guard only on NNIs or on enhanced network interfaces ENIs on which STP has been enabled. To set a port as an NNI or ENI, enter the **port-type** {nni | eni} interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

You can enable root guard or loop guard when the switch is operating in the per-VLAN spanning-tree plus (PVST+), the rapid-PVST+, or the multiple spanning-tree (MST) mode.

When root guard is enabled, if spanning-tree calculations cause an interface to be selected as the root port, the interface transitions to the root-inconsistent (blocked) state to prevent the customer's switch from becoming the root switch or being in the path to the root. The root port provides the best path from the switch to the root switch.

When the **no spanning-tree guard** or the **no spanning-tree guard none** command is entered, root guard is disabled for all VLANs on the selected NNI. If this interface is in the root-inconsistent (blocked) state, it automatically transitions to the listening state.

Loop guard is most effective when it is configured on the entire switched network. When the switch is operating in PVST+ or rapid-PVST+ mode, loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send bridge protocol data units (BPDUs) on root or alternate ports. When the switch is operating in MST mode, BPDUs are not sent on nonboundary interfaces if the interface is blocked by loop guard in all MST instances. On a boundary interface, loop guard blocks the interface in all MST instances.

To disable root guard or loop guard, use the **spanning-tree guard none** interface configuration command on an STP interface. You cannot enable both root guard and loop guard at the same time.

You can override the setting of the **spanning-tree loopguard default** global configuration command by using the **spanning-tree guard loop** interface configuration command on an STP interface.

### Examples

This example shows how to enable root guard on all the VLANs associated with the specified port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree guard root
```

This example shows how to enable loop guard on all the VLANs associated with the specified port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree guard loop
```

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

### Related Commands

Command	Description
<b>show running-config</b>	Displays the operating configuration.
<b>spanning-tree cost</b>	Sets the path cost for spanning-tree calculations.
<b>spanning-tree loopguard default</b>	Prevents alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link.
<b>spanning-tree mst cost</b>	Configures the path cost for MST calculations.
<b>spanning-tree mst port-priority</b>	Configures an STP MST port priority.
<b>spanning-tree mst root</b>	Configures the MST root switch priority and timers based on the network diameter.
<b>spanning-tree port-priority</b>	Configures an STP port priority.
<b>spanning-tree vlan priority</b>	Sets the switch priority for the specified spanning-tree instance.

## spanning-tree link-type

Use the **spanning-tree link-type** interface configuration command on a network node interface (NNI) or enhanced network interface (ENI) with STP enabled to override the default link-type setting, which is determined by the duplex mode of the STP port, and to enable rapid spanning-tree transitions to the forwarding state. Use the **no** form of this command to return to the default setting.

**spanning-tree link-type { point-to-point | shared }**

**no spanning-tree link-type**

### Syntax Description

<b>point-to-point</b>	Specify that the link type of an STP port is point-to-point.
<b>shared</b>	Specify that the link type of an STP port is shared.

### Defaults

The switch derives the link type of an interface from the duplex mode. A full-duplex interface is considered a point-to-point link, and a half-duplex interface is considered a shared link.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). You can configure spanning-tree link type only on NNIs or on ENIs on which STP has been enabled. To set a port as an NNI or ENI, enter the **port-type { eni | nni }** interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

You can override the default setting of the link type by using the **spanning-tree link-type** command. For example, a half-duplex link can be physically connected point-to-point to a single interface on a remote switch running the Multiple Spanning Tree Protocol (MSTP) or the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol and be enabled for rapid transitions.

### Examples

This example shows how to specify the link type as shared (regardless of the duplex setting) and to prevent rapid transitions to the forwarding state:

```
Switch(config-if)# spanning-tree link-type shared
```

You can verify your setting by entering the **show spanning-tree mst interface interface-id** or the **show spanning-tree interface interface-id** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>clear spanning-tree detected-protocols</b>	Restarts the protocol migration process (force the renegotiation with neighboring switches) on all interfaces or on the specified interface.
<b>show spanning-tree interface</b> <i>interface-id</i>	Displays spanning-tree state information for the specified interface.
<b>show spanning-tree mst interface</b> <i>interface-id</i>	Displays MST information for the specified interface.

# spanning-tree loopguard default

Use the **spanning-tree loopguard default** global configuration command to enable loopguard by default on all network node interfaces (NNIs) or enhanced network interface (ENIs) with STP enabled. Enabling loopguard prevents alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link. Use the **no** form of this command to return to the default setting.

**spanning-tree loopguard default**

**no spanning-tree loopguard default**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Loop guard is disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** Spanning Tree Protocol (STP) is supported only on NNIs or on ENIs on which STP has been enabled. To set a port as an NNI or ENI, enter the **port-type {eni | nni}** interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

This command has no effect on user network interfaces (UNIs).

You can enable the loop guard feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode.

Loop guard is most effective when it is configured on the entire switched network. When the switch is operating in PVST+ or rapid-PVST+ mode, loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send bridge protocol data units (BPDUs) on root or alternate ports. When the switch is operating in MST mode, BPDUs are not sent on nonboundary interfaces if the interface is blocked by loop guard in all MST instances. On a boundary interface, loop guard blocks the interface in all MST instances.

Loop guard operates only on STP ports that the spanning tree identifies as point-to-point.

You can override the setting of the **spanning-tree loopguard default** global configuration command by using the **spanning-tree guard loop** interface configuration command.

**Examples** This example shows how to globally enable loop guard:

```
Switch(config)# spanning-tree loopguard default
```

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

Related Commands	Command	Description
	<b>show running-config</b>	Displays the operating configuration.
	<b>spanning-tree guard loop</b>	Enables the loop guard feature on all the VLANs associated with the specified STP port.

# spanning-tree mode

Use the **spanning-tree mode** global configuration command to enable per-VLAN spanning-tree plus (PVST+), rapid PVST+, or multiple spanning tree (MST) on your switch. Use the **no** form of this command to return to the default setting.

**spanning-tree mode {mst | pvst | rapid-pvst}**

**no spanning-tree mode**

## Syntax Description

<b>mst</b>	Enable MST and Rapid Spanning Tree Protocol (RSTP) (based on IEEE 802.1s and IEEE 802.1w).
<b>pvst</b>	Enable PVST+ (based on IEEE 802.1D).
<b>rapid-pvst</b>	Enable rapid PVST+ (based on IEEE 802.1w).

## Defaults

The default mode is rapid PVST+.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

Spanning Tree Protocol (STP) is supported on the switch only on network node interfaces (NNIs) or on enhanced network interfaces (ENIs) on which STP has been enabled. To set a port as an NNI or ENI, enter the **port-type {eni | nni}** interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

STP is not supported on user network interfaces (UNIs).

The switch supports PVST+, rapid PVST+, and MSTP, but only one version can be active at any time: All VLANs run PVST+, all VLANs run rapid PVST+, or all VLANs run MSTP.

When you enable the MST mode, RSTP is automatically enabled.



### Caution

Changing spanning-tree modes can disrupt traffic because all spanning-tree instances are stopped for the previous mode and restarted in the new mode.

## Examples

This example shows to enable MST and RSTP on the switch:

```
Switch(config)# spanning-tree mode mst
```

This example shows to enable PVST+ on the switch:

```
Switch(config)# spanning-tree mode pvst
```



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

Related Commands	Command	Description
	<b>show running-config</b>	Displays the operating configuration.

# spanning-tree mst configuration

Use the **spanning-tree mst configuration** global configuration command to enter multiple spanning-tree (MST) configuration mode through which you configure the MST region. Use the **no** form of this command to return to the default settings.

**spanning-tree mst configuration**

**no spanning-tree mst configuration**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The default mapping is that all VLANs are mapped to the common and internal spanning-tree (CIST) instance (instance 0).

The default name is an empty string.

The revision number is 0.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

On the Cisco ME switch, spanning-tree MST configuration is supported only on network node interfaces (NNIs) or on enhanced network interfaces (ENIs) on which STP has been enabled. To set a port as an NNI or ENI, enter the **port-type {eni | nni}** interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

User network interfaces (UNIs) do not participate in Spanning Tree Protocol (STP).

The **spanning-tree mst configuration** command enables the MST configuration mode. These configuration commands are available:

- **abort**: exits the MST region configuration mode without applying configuration changes.
- **exit**: exits the MST region configuration mode and applies all configuration changes.
- **instance** *instance-id* **vlan** *vlan-range*: maps VLANs to an MST instance. The range for the *instance-id* is 0 to 4094. The range for *vlan-range* is 1 to 4094. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma.
- **name** *name*: sets the configuration name. The *name* string has a maximum length of 32 characters and is case sensitive.
- **no**: negates the **instance**, **name**, and **revision** commands or sets them to their defaults.
- **private-vlan**: Though visible in the command-line help strings, this command is not supported.

- **revision** *version*: sets the configuration revision number. The range is 0 to 65535.
- **show [current | pending]**: displays the current or pending MST region configuration.

In MST mode, the switch supports up to 16 MST instances. The number of VLANs that can be mapped to a particular MST instance is unlimited.

When you map VLANs to an MST instance, the mapping is incremental, and VLANs specified in the command are added to or removed from the VLANs that were previously mapped. To specify a range, use a hyphen; for example, **instance 1 vlan 1-63** maps VLANs 1 to 63 to MST instance 1. To specify a series, use a comma; for example, **instance 1 vlan 10, 20, 30** maps VLANs 10, 20, and 30 to MST instance 1.

All VLANs that are not explicitly mapped to an MST instance are mapped to the common and internal spanning tree (CIST) instance (instance 0) and cannot be unmapped from the CIST by using the **no** form of the command.

For two or more switches to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number, and the same name.

### Examples

This example shows how to enter MST configuration mode, map VLANs 10 to 20 to MST instance 1, name the region *region1*, set the configuration revision to 1, display the pending configuration, apply the changes, and return to global configuration mode:

```
Switch# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name region1
Switch(config-mst)# revision 1
Switch(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
-----  -
0         1-9,21-4094
1         10-20
-----  -

Switch(config-mst)# exit
Switch(config)#
```

This example shows how to add VLANs 1 to 100 to the ones already mapped (if any) to instance 2, to move VLANs 40 to 60 that were previously mapped to instance 2 to the CIST instance, to add VLAN 10 to instance 10, and to remove all the VLANs mapped to instance 2 and map them to the CIST instance:

```
Switch(config-mst)# instance 2 vlan 1-100
Switch(config-mst)# no instance 2 vlan 40-60
Switch(config-mst)# instance 10 vlan 10
Switch(config-mst)# no instance 2
```

You can verify your settings by entering the **show pending** MST configuration command.

### Related Commands

Command	Description
<b>show spanning-tree mst configuration</b>	Displays the MST region configuration.

## spanning-tree mst cost

Use the **spanning-tree mst cost** interface configuration command on a network node interface (NNI) or an enhanced network interface (ENI) with STP enabled to set the path cost for multiple spanning-tree (MST) calculations. If a loop occurs, spanning tree considers the path cost when selecting an interface to put in the forwarding state. Use the **no** form of this command to return to the default setting.

**spanning-tree mst** *instance-id* **cost** *cost*

**no spanning-tree mst** *instance-id* **cost**

Syntax Description	instance-id	cost
	Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094.	Path cost is 1 to 200000000, with higher values meaning higher costs.

**Defaults** The default path cost is computed from the interface bandwidth setting. These are the IEEE default path cost values:

- 1000 Mbps—20000
- 100 Mbps—200000
- 10 Mbps—2000000

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). You can configure path cost only on NNIs or on ENIs on which STP has been enabled. To set a port as an NNI or ENI, enter the **port-type {eni | nni}** interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

When you configure the cost, higher values represent higher costs.

**Examples** This example shows how to set a path cost of 250 on a port associated with instances 2 and 4:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree mst 2,4 cost 250
```

You can verify your settings by entering the **show spanning-tree mst interface interface-id** privileged EXEC command.

Related Commands	Command	Description
	<b>show spanning-tree mst</b> <b>interface</b> <i>interface-id</i>	Displays MST information for the specified interface.
	<b>spanning-tree mst</b> <b>port-priority</b>	Configures an interface priority.
	<b>spanning-tree mst priority</b>	Configures the switch priority for the specified spanning-tree instance.

## spanning-tree mst forward-time

Use the **spanning-tree mst forward-time** global configuration command to set the forward-delay time for all multiple spanning-tree (MST) instances. The forwarding time specifies how long each of the listening and learning states last before the interface begins forwarding. Use the **no** form of this command to return to the default setting.

**spanning-tree mst forward-time** *seconds*

**no spanning-tree mst forward-time**

<b>Syntax Description</b>	<i>seconds</i>	Length of the listening and learning states. The range is 4 to 30 seconds.
---------------------------	----------------	--

<b>Defaults</b>	The default is 15 seconds.
-----------------	----------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

<b>Usage Guidelines</b>	<p>On the Cisco ME switch, spanning-tree MST configuration is supported only on network node interfaces (NNIs) or on enhanced network interfaces (ENIs) on which Spanning-Tree Protocol (STP) has been enabled. To set a port as an NNI or ENI, enter the <b>port-type { nni   eni }</b> interface configuration command. To enable STP on an ENI, enter the <b>spanning-tree</b> interface configuration command.</p>
-------------------------	--

User network interfaces (UNIs) do not participate in STP.

Changing the **spanning-tree mst forward-time** command affects all spanning-tree instances.

<b>Examples</b>	This example shows how to set the spanning-tree forwarding time to 18 seconds for all MST instances:
-----------------	--

```
Switch(config)# spanning-tree mst forward-time 18
```

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show spanning-tree mst</a>	Displays MST information.
	<a href="#">spanning-tree mst hello-time</a>	Sets the interval between hello bridge protocol data units (BPDUs) sent by root switch configuration messages.
	<a href="#">spanning-tree mst max-age</a>	Sets the interval between messages that the spanning tree receives from the root switch.
	<a href="#">spanning-tree mst max-hops</a>	Sets the number of hops in a region before the BPDU is discarded.

# spanning-tree mst hello-time

Use the **spanning-tree mst hello-time** global configuration command to set the interval between hello bridge protocol data units (BPDUs) sent by root switch configuration messages. Use the **no** form of this command to return to the default setting.

**spanning-tree mst hello-time** *seconds*

**no spanning-tree mst hello-time**

<b>Syntax Description</b>	<i>seconds</i>	Interval between hello BPDUs sent by root switch configuration messages. The range is 1 to 10 seconds.
---------------------------	----------------	--

<b>Defaults</b>	The default is 2 seconds.
-----------------	---------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

**Usage Guidelines**

On the Cisco ME switch, spanning-tree MST configuration is supported only on network node interfaces (NNIs) or on enhanced network interfaces (ENIs) on which Spanning-Tree Protocol (STP) has been enabled. To set a port as an NNI or ENI, enter the **port-type {eni | nni}** interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

User network interfaces (UNIs) do not participate in STP.

After you set the **spanning-tree mst max-age** *seconds* global configuration command, if a switch does not receive BPDUs from the root switch within the specified interval, the switch recomputes the spanning-tree topology. The **max-age** setting must be greater than the **hello-time** setting.

Changing the **spanning-tree mst hello-time** command affects all spanning-tree instances.

**Examples**

This example shows how to set the spanning-tree hello time to 3 seconds for all multiple spanning-tree (MST) instances:

```
Switch(config)# spanning-tree mst hello-time 3
```

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">show spanning-tree mst</a>	Displays MST information.
	<a href="#">spanning-tree mst forward-time</a>	Sets the forward-delay time for all MST instances.
	<a href="#">spanning-tree mst max-age</a>	Sets the interval between messages that the spanning tree receives from the root switch.
	<a href="#">spanning-tree mst max-hops</a>	Sets the number of hops in a region before the BPDU is discarded.



## spanning-tree mst max-age

Use the **spanning-tree mst max-age** global configuration command to set the interval between messages that the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputes the spanning-tree topology. Use the **no** form of this command to return to the default setting.

**spanning-tree mst max-age** *seconds*

**no spanning-tree mst max-age**

<b>Syntax Description</b>	<i>seconds</i>	Interval between messages the spanning tree receives from the root switch. The range is 6 to 40 seconds.
---------------------------	----------------	--

<b>Defaults</b>	The default is 20 seconds.
-----------------	----------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

**Usage Guidelines**

On the Cisco ME switch, spanning-tree MST configuration is supported only on network node interfaces (NNIs) or on enhanced network interfaces (ENIs) on which Spanning Tree Protocol (STP) has been enabled. To set a port as an NNI or ENI, enter the **port-type {eni | nni}** interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

User network interfaces (UNIs) do not participate in STP.

After you set the **spanning-tree mst max-age seconds** global configuration command, if a switch does not receive BPDUs from the root switch within the specified interval, the switch recomputes the spanning-tree topology. The **max-age** setting must be greater than the **hello-time** setting.

Changing the **spanning-tree mst max-age** command affects all spanning-tree instances.

**Examples**

This example shows how to set the spanning-tree max-age to 30 seconds for all multiple spanning-tree (MST) instances:

```
Switch(config)# spanning-tree mst max-age 30
```

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">show spanning-tree mst</a>	Displays MST information.
	<a href="#">spanning-tree mst forward-time</a>	Sets the forward-delay time for all MST instances.
	<a href="#">spanning-tree mst hello-time</a>	Sets the interval between hello BPDUs sent by root switch configuration messages.
	<a href="#">spanning-tree mst max-hops</a>	Sets the number of hops in a region before the BPDU is discarded.

## spanning-tree mst max-hops

Use the **spanning-tree mst max-hops** global configuration command to set the number of hops in a region before the bridge protocol data unit (BPDU) is discarded and the information held for an interface is aged. Use the **no** form of this command to return to the default setting.

**spanning-tree mst max-hops** *hop-count*

**no spanning-tree mst max-hops**

<b>Syntax Description</b>	<i>hop-count</i> Number of hops in a region before the BPDU is discarded. The range is 1 to 255 hops.
---------------------------	---

<b>Defaults</b>	The default is 20 hops.
-----------------	-------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

<b>Usage Guidelines</b>	<p>On the Cisco ME switch, spanning-tree MST configuration is supported only on network node interfaces (NNIs) or on enhanced network interfaces (ENIs) on which Spanning Tree Protocol (STP) has been enabled. To set a port as an NNI or ENI, enter the <b>port-type {eni   nni}</b> interface configuration command. To enable STP on an ENI, enter the <b>spanning-tree</b> interface configuration command.</p>
-------------------------	--

User network interfaces (UNIs) do not participate in STP.

The root switch of the instance always sends a BPDU (or M-record) with a cost of 0 and the hop count set to the maximum value. When a switch receives this BPDU, it decrements the received remaining hop count by one and propagates the decremented count as the remaining hop count in the generated M-records. A switch discards the BPDU and ages the information held for the interface when the count reaches 0.

Changing the **spanning-tree mst max-hops** command affects all spanning-tree instances.

<b>Examples</b>	This example shows how to set the spanning-tree max-hops to 10 for all multiple spanning-tree (MST) instances:
-----------------	--

```
Switch(config)# spanning-tree mst max-hops 10
```

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">show spanning-tree mst</a>	Displays MST information.
	<a href="#">spanning-tree mst forward-time</a>	Sets the forward-delay time for all MST instances.
	<a href="#">spanning-tree mst hello-time</a>	Sets the interval between hello BPDU sent by root switch configuration messages.
	<a href="#">spanning-tree mst max-age</a>	Sets the interval between messages that the spanning tree receives from the root switch.

## spanning-tree mst port-priority

Use the **spanning-tree mst port-priority** interface configuration command on a network node interface (NNI) or enhanced network interface (ENI) with STP enabled to configure an interface priority. If a loop occurs, the Multiple Spanning Tree Protocol (MSTP) can find the interface to put in the forwarding state. Use the **no** form of this command to return to the default setting.

**spanning-tree mst** *instance-id* **port-priority** *priority*

**no spanning-tree mst** *instance-id* **port-priority**

Syntax Description	
<i>instance-id</i>	Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094.
<i>priority</i>	The range is 0 to 240 in increments of 16. Valid priority values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected. The lower the number, the higher the priority.

### Defaults

The default is 128.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). You can configure spanning-tree MST port priority only on NNIs or on ENIs on which STP has been enabled. To set a port as an ENI or NNI, enter the **port-type** {**eni** | **nni**} interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

You can assign higher priority values (lower numerical values) to STP port that you want selected first and lower priority values (higher numerical values) that you want selected last. If all STP ports have the same priority value, the multiple spanning tree (MST) puts the interface with the lowest interface number in the forwarding state and blocks other interfaces.

### Examples

This example shows how to increase the likelihood that the interface associated with spanning-tree instances 20 and 22 is placed into the forwarding state if a loop occurs:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree mst 20,22 port-priority 0
```

You can verify your settings by entering the **show spanning-tree mst interface** *interface-id* privileged EXEC command.

Related Commands	Command	Description
	<code>show spanning-tree mst interface interface-id</code>	Displays MST information for the specified interface.
	<code>spanning-tree mst cost</code>	Sets the path cost for MST calculations.
	<code>spanning-tree mst priority</code>	Sets the switch priority for the specified spanning-tree instance.

# spanning-tree mst pre-standard

Use the **spanning-tree mst pre-standard** interface configuration command to configure a port to send only prestandard bridge protocol data units (BPDUs).

**spanning-tree mst pre-standard**

**no spanning-tree mst pre-standard**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The default state is automatic detection of prestandard neighbors.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The port can accept both prestandard and standard BPDUs. If the neighbor types are mismatched, only the common and internal spanning tree (CIST) runs on this interface.



### Note

If a switch port is connected to a switch running prestandard Cisco IOS software, you *must* use the **spanning-tree mst pre-standard** interface configuration command on the port. If you do not configure the port to send only prestandard BPDUs, the Multiple STP (MSTP) performance might diminish.

When the port is configured to automatically detect prestandard neighbors, the *prestandard* flag always appears in the **show spanning-tree mst** commands.

## Examples

This example shows how to configure a port to send only prestandard BPDUs:

```
Switch(config-if)# spanning-tree mst pre-standard
```

You can verify your settings by entering the **show spanning-tree mst** privileged EXEC command.

## Related Commands

Command	Description
<b>show spanning-tree mst</b> <i>instance-id</i>	Displays multiple spanning-tree (MST) information, including the <i>prestandard</i> flag, for the specified interface.

## spanning-tree mst priority

Use the **spanning-tree mst priority** global configuration command to set the switch priority for the specified spanning-tree instance. Use the **no** form of this command to return to the default setting.

**spanning-tree mst** *instance-id* **priority** *priority*

**no spanning-tree mst** *instance-id* **priority**

<b>Syntax Description</b>	<i>instance-id</i>	Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094.
	<b>priority</b>	Set the switch priority for the specified spanning-tree instance. This setting affects the likelihood that the switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch.  The range is 0 to 61440 in increments of 4096. Valid priority values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.

**Defaults** The default is 32768.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs); it is only supported on network node interfaces (NNIs) or on enhanced network interfaces (ENIs) on which STP has been enabled. To set a port as an ENI or NNI, enter the **port-type** {eni | nni} interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

**Examples** This example shows how to set the spanning-tree priority to 8192 for multiple spanning-tree instances (MST) 20 to 21:

```
Switch(config)# spanning-tree mst 20-21 priority 8192
```

You can verify your settings by entering the **show spanning-tree mst instance-id** privileged EXEC command.



Related Commands	Command	Description
	<a href="#">show spanning-tree mst <i>instance-id</i></a>	Displays MST information for the specified interface.
	<a href="#">spanning-tree mst cost</a>	Sets the path cost for MST calculations.
	<a href="#">spanning-tree mst port-priority</a>	Configures an interface priority.

## spanning-tree mst root

Use the **spanning-tree mst root** global configuration command to configure the multiple spanning-tree (MST) root switch priority and timers based on the network diameter. Use the **no** form of this command to return to the default settings.

```
spanning-tree mst instance-id root { primary | secondary } [diameter net-diameter
[hello-time seconds]]
```

```
no spanning-tree mst instance-id root
```

### Syntax Description

<i>instance-id</i>	Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094.
<b>root primary</b>	Force this switch to be the root switch.
<b>root secondary</b>	Set this switch to be the root switch should the primary root switch fail.
<b>diameter</b> <i>net-diameter</i>	(Optional) Set the maximum number of switches between any two end stations. The range is 2 to 7. This keyword is available only for MST instance 0.
<b>hello-time</b> <i>seconds</i>	(Optional) Set the interval between hello bridge protocol data units (BPDUs) sent by the root switch configuration messages. The range is 1 to 10 seconds. This keyword is available only for MST instance 0.

### Defaults

The primary root switch priority is 24576.

The secondary root switch priority is 28672.

The hello time is 2 seconds.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs); it is only supported on network node interfaces (NNIs) or on enhanced network interfaces (ENIs) on which STP has been enabled. To set a port as an ENI or NNI, enter the **port-type** { **eni** | **nni** } interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

Use the **spanning-tree mst** *instance-id* **root** command only on backbone switches.

When you enter the **spanning-tree mst *instance-id* root** command, the software tries to set a high enough priority to make this switch the root of the spanning-tree instance. Because of the extended system ID support, the switch sets the switch priority for the instance to 24576 if this value will cause this switch to become the root for the specified instance. If any root switch for the specified instance has a switch priority lower than 24576, the switch sets its own priority to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value.)

When you enter the **spanning-tree mst *instance-id* root secondary** command, because of support for the extended system ID, the software changes the switch priority from the default value (32768) to 28672. If the root switch fails, this switch becomes the next root switch (if the other switches in the network use the default switch priority of 32768 and are therefore unlikely to become the root switch).

### Examples

This example shows how to configure the switch as the root switch for instance 10 with a network diameter of 4:

```
Switch(config)# spanning-tree mst 10 root primary diameter 4
```

This example shows how to configure the switch as the secondary root switch for instance 10 with a network diameter of 4:

```
Switch(config)# spanning-tree mst 10 root secondary diameter 4
```

You can verify your settings by entering the **show spanning-tree mst *instance-id*** privileged EXEC command.

### Related Commands

Command	Description
<b>show spanning-tree mst <i>instance-id</i></b>	Displays MST information for the specified instance.
<b>spanning-tree mst forward-time</b>	Sets the forward-delay time for all MST instances.
<b>spanning-tree mst hello-time</b>	Sets the interval between hello BPDUs sent by root switch configuration messages.
<b>spanning-tree mst max-age</b>	Sets the interval between messages that the spanning tree receives from the root switch.
<b>spanning-tree mst max-hops</b>	Sets the number of hops in a region before the BPDU is discarded.

## spanning-tree port-priority

Use the **spanning-tree port-priority** interface configuration command on a network node interface (NNI) or an enhanced network interface (ENI) on which Spanning Tree Protocol (STP) has been enabled to configure an interface priority. If a loop occurs, spanning tree can find the interface to put in the forwarding state. Use the **no** form of this command to return to the default setting.

**spanning-tree** [**vlan** *vlan-id*] **port-priority** *priority*

**no spanning-tree** [**vlan** *vlan-id*] **port-priority**

Syntax Description	
<b>vlan</b> <i>vlan-id</i>	(Optional) VLAN range associated with a spanning-tree instance. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
<i>priority</i>	Number from 0 to 240, in increments of 16. Valid values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected. The lower the number, the higher the priority.

**Defaults** The default is 128.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** STP is not supported on user network interfaces (UNIs). You can configure spanning-tree port priority only on NNIs or on ENIs on which STP has been enabled. To set a port as an ENI or NNI, enter the **port-type** {**eni** | **nni**} interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

If the variable *vlan-id* is omitted, the command applies to the spanning-tree instance associated with VLAN 1.

You can set the priority on a VLAN that has no interfaces assigned to it. The setting takes effect when you assign the STP port to the VLAN.

If you configure an STP port with both the **spanning-tree vlan** *vlan-id* **port-priority** *priority* command and the **spanning-tree port-priority** *priority* command, the **spanning-tree vlan** *vlan-id* **port-priority** *priority* command takes effect.

**Examples** This example shows how to increase the likelihood that a port will be put in the forwarding state if a loop occurs:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree vlan 20 port-priority 0
```

This example shows how to set the port-priority value on VLANs 20 to 25:

```
Switch(config-if)# spanning-tree vlan 20-25 port-priority 0
```

You can verify your settings by entering the **show spanning-tree interface** *interface-id* privileged EXEC command.

Related Commands	Command	Description
	<b>show spanning-tree interface</b> <i>interface-id</i>	Displays spanning-tree information for the specified interface.
	<b>spanning-tree cost</b>	Sets the path cost for spanning-tree calculations.
	<b>spanning-tree vlan priority</b>	Sets the switch priority for the specified spanning-tree instance.

## spanning-tree portfast (global configuration)

Use the **spanning-tree portfast** global configuration command to globally enable bridge protocol data unit (BPDU) filtering on Port Fast-enabled network node interfaces (NNIs) or enhanced network interfaces (ENIs) on which Spanning Tree Protocol (STP) has been enabled, to enable the BPDU guard feature on Port Fast-enabled STP ports, or the Port Fast feature on all nontrunking STP ports. The BPDU filtering feature prevents the switch STP port from sending or receiving BPDUs. The BPDU guard feature puts Port Fast-enabled STP ports that receive BPDUs in an error-disabled state. Use the **no** form of this command to return to the default settings.

**spanning-tree portfast { bpdupfilter default | bpduguard default | default }**

**no spanning-tree portfast { bpdupfilter default | bpduguard default | default }**

Syntax Description		
	<b>bpdupfilter default</b>	Globally enable BPDU filtering on Port Fast-enabled STP ports, and prevent the switch STP port connected to end stations from sending or receiving BPDUs.
	<b>bpduguard default</b>	Globally enable the BPDU guard feature on Port Fast-enabled STP ports, and place the STP ports that receive BPDUs in an error-disabled state.
	<b>default</b>	Globally enable the Port Fast feature on all nontrunking STP ports. When the Port Fast feature is enabled, the STP port changes directly from a blocking state to a forwarding state without making the intermediate spanning-tree state changes.

**Defaults** The BPDU filtering, the BPDU guard, and the Port Fast features are disabled on all NNIs or ENIs unless they are individually configured.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** STP is not supported on user network interfaces (UNIs) on the switch. Spanning-tree configuration affects only NNIs or ENIs on which STP has been enabled. To set a port as an ENI or NNI, enter the **port-type { eni | nni }** interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

UNIs are typically customer-facing ports and do not participate in the spanning tree of the service provider. However, if you configure a customer-facing port as an ENI and enable spanning tree, the ENI could become the spanning tree root port unless you configure root guard on the port by using the **spanning-tree guard root** interface configuration command. A customer-facing ENI with STP enabled participates in the same spanning tree as the service-provider facing NNI.

**Note**

Exercise caution when enabling STP on a customer-facing ENI.

You can enable these features when the switch is operating in the per-VLAN spanning-tree plus (PVST+), the rapid-PVST+, or the multiple spanning-tree (MST) mode.

Use the **spanning-tree portfast bpdudfilter default** global configuration command to globally enable BPDU filtering on STP ports that are Port Fast-enabled. The STP ports 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 STP ports do not receive BPDUs. If a BPDU is received on a Port Fast-enabled STP port, the interface loses its Port Fast-operational status and BPDU filtering is disabled.

You can override the **spanning-tree portfast bpdudfilter default** global configuration command on an STP port by using the **spanning-tree bpdudfilter** interface configuration command.

**Caution**

Enabling BPDU filtering on an STP port is the same as disabling spanning tree on it and can result in spanning-tree loops.

Use the **spanning-tree portfast bpduguard default** global configuration command to globally enable BPDU guard on STP ports that are in a Port Fast-operational state. In a valid configuration, Port Fast-enabled STP ports do not receive BPDUs. Receiving a BPDU on a Port Fast-enabled STP port signals an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the STP port in the error-disabled state. The BPDU guard feature provides a secure response to invalid configurations because you must manually put the STP port back in service. Use the BPDU guard feature in a service-provider network to prevent an access port from participating in the spanning tree.

You can override the **spanning-tree portfast bpduguard default** global configuration command by using the **spanning-tree bpduguard** interface configuration command on an STP port.

Use the **spanning-tree portfast default** global configuration command to globally enable the Port Fast feature on all nontrunking STP ports. Configure Port Fast only on STP ports that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation. A Port Fast-enabled STP port moves directly to the spanning-tree forwarding state when linkup occurs without waiting for the standard forward-delay time.

You can override the **spanning-tree portfast default** global configuration command by using the **spanning-tree portfast** interface configuration command on an STP port. You can use the **no spanning-tree portfast default** global configuration command to disable Port Fast on all STP ports unless they are individually configured with the **spanning-tree portfast** interface configuration command.

**Examples**

This example shows how to globally enable the BPDU filtering feature:

```
Switch(config)# spanning-tree portfast bpdudfilter default
```

This example shows how to globally enable the BPDU guard feature:

```
Switch(config)# spanning-tree portfast bpduguard default
```

This example shows how to globally enable the Port Fast feature on all nontrunking interfaces:

```
Switch(config)# spanning-tree portfast default
```

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

Related Commands	Command	Description
	<b>show running-config</b>	Displays the operating configuration.
	<a href="#">spanning-tree bpdupfilter</a>	Prevents an interface from sending or receiving BPDUs.
	<a href="#">spanning-tree bpduguard</a>	Puts an STP port in the error-disabled state when it receives a BPDU.
	<a href="#">spanning-tree portfast (interface configuration)</a>	Enables the Port Fast feature on an STP port in all its associated VLANs.



## spanning-tree portfast (interface configuration)

Use the **spanning-tree portfast** interface configuration command on a network node interface (NNI) or an enhanced network interface (ENI) on which Spanning Tree Protocol (STP) has been enabled to enable the Port Fast feature on an STP port in all its associated VLANs. When the Port Fast feature is enabled, the STP port changes directly from a blocking state to a forwarding state without making the intermediate spanning-tree state changes. Use the **no** form of this command to return to the default setting.

**spanning-tree portfast** [**disable** | **trunk**]

**no spanning-tree portfast**

Syntax Description	disable	(Optional) Disable the Port Fast feature on the specified interface.
	<b>trunk</b>	(Optional) Enable the Port Fast feature on a trunking interface.

**Defaults** The Port Fast feature is disabled on all ports.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** STP is not supported on user network interfaces (UNIs). You can enable the spanning-tree Port Fast feature only on NNIs or on ENIs on which STP has been enabled. To set a port as an NNI or ENI, enter the **port-type** {**nni** | **eni**} interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

Use this feature only on STP ports that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation.

To enable Port Fast on trunk ports, you must use the **spanning-tree portfast trunk** interface configuration command. The **spanning-tree portfast** command is not supported on trunk ports.

You can enable this feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), the rapid-PVST+, or the multiple spanning-tree (MST) mode.

This feature affects all VLANs on the STP port.

An NNI with the Port Fast feature enabled is moved directly to the spanning-tree forwarding state without the standard forward-time delay.

You can use the **spanning-tree portfast default** global configuration command to globally enable the Port Fast feature on all nontrunking interfaces. However, the **spanning-tree portfast** interface configuration command can override the global setting.

**spanning-tree portfast (interface configuration)**

If you configure the **spanning-tree portfast default** global configuration command, you can disable Port Fast on an STP port that is not a trunk interface by using the **spanning-tree portfast disable** interface configuration command.

**Examples**

This example shows how to enable the Port Fast feature on a port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree portfast
```

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

**Related Commands**

Command	Description
<b>show running-config</b>	Displays the operating configuration.
<b>spanning-tree bpdupfilter</b>	Prevents an interface from sending or receiving bridge protocol data units (BPDUs).
<b>spanning-tree bpduguard</b>	Puts an interface in the error-disabled state when it receives a BPDU.
<b>spanning-tree portfast (global configuration)</b>	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled STP ports or enables the Port Fast feature on all nontrunking STP ports.

## spanning-tree vlan

Use the **spanning-tree vlan** global configuration command to configure spanning tree on a per-VLAN basis. Use the **no** form of this command to return to the default setting.

```
spanning-tree vlan vlan-id [forward-time seconds | hello-time seconds | max-age seconds |
priority priority | root {primary | secondary} [diameter net-diameter
hello-time seconds]]]
```

```
no spanning-tree vlan vlan-id [forward-time | hello-time | max-age | priority | root]
```

### Syntax Description

<i>vlan-id</i>	VLAN range associated with a spanning-tree instance. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
<b>forward-time</b> <i>seconds</i>	(Optional) Set the forward-delay time for the specified spanning-tree instance. The forwarding time specifies how long each of the listening and learning states last before the interface begins forwarding. The range is 4 to 30 seconds.
<b>hello-time</b> <i>seconds</i>	(Optional) Set the interval between hello bridge protocol data units (BPDUs) sent by the root switch configuration messages. The range is 1 to 10 seconds.
<b>max-age</b> <i>seconds</i>	(Optional) Set the interval between messages the spanning tree receives from the root switch. If a switch does not receive a BPDU message from the root switch within this interval, it recomputes the spanning-tree topology. The range is 6 to 40 seconds.
<b>priority</b> <i>priority</i>	(Optional) Set the switch priority for the specified spanning-tree instance. This setting affects the likelihood that this switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch.  The range is 0 to 61440 in increments of 4096. Valid priority values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.
<b>root primary</b>	(Optional) Force this switch to be the root switch.
<b>root secondary</b>	(Optional) Set this switch to be the root switch should the primary root switch fail.
<b>diameter</b> <i>net-diameter</i>	(Optional) Set the maximum number of switches between any two end stations. The range is 2 to 7.

### Defaults

Spanning tree is enabled on all VLANs.

The forward-delay time is 15 seconds.

The hello time is 2 seconds.

The max-age is 20 seconds.

The primary root switch priority is 24576.

The secondary root switch priority is 28672.

**Command Modes** Global configuration

**Command History**

Release	Modification
12.2(44)EY	This command was introduced.

**Usage Guidelines**

The switch does not support Spanning Tree Protocol (STP) on user network interfaces (UNIs). Only the switch network node interfaces (NNIs) or STP-enabled enhanced network interfaces (ENIs) in a VLAN participate in STP.

Disabling the STP causes the VLAN to stop participating in the spanning-tree topology. STP ports that are administratively down remain down. Received BPDUs are forwarded like other multicast frames. The VLAN does not detect and prevent loops when STP is disabled.

You can disable the STP on a VLAN that is not currently active and verify the change by using the **show running-config** or the **show spanning-tree vlan *vlan-id*** privileged EXEC command. The setting takes effect when the VLAN is activated.

When disabling or re-enabling the STP, you can specify a range of VLANs that you want to disable or enable.

When a VLAN is disabled and then enabled, all assigned VLANs continue to be its members. However, all spanning-tree bridge parameters are returned to their previous settings (the last setting before the VLAN was disabled).

You can enable spanning-tree options on a VLAN that has no STP ports assigned to it. The setting takes effect when you assign interfaces to it.

When setting the **max-age *seconds***, if a switch does not receive BPDUs from the root switch within the specified interval, it recomputes the spanning-tree topology. The **max-age** setting must be greater than the **hello-time** setting.

The **spanning-tree vlan *vlan-id* root** command should be used only on backbone switches.

When you enter the **spanning-tree vlan *vlan-id* root** command, the software checks the switch priority of the current root switch for each VLAN. Because of the extended system ID support, the switch sets the switch priority for the specified VLAN to 24576 if this value will cause this switch to become the root for the specified VLAN. If any root switch for the specified VLAN has a switch priority lower than 24576, the switch sets its own priority for the specified VLAN to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value.)

When you enter the **spanning-tree vlan *vlan-id* root secondary** command, because of support for the extended system ID, the software changes the switch priority from the default value (32768) to 28672. If the root switch should fail, this switch becomes the next root switch (if the other switches in the network use the default switch priority of 32768, and therefore, are unlikely to become the root switch).

**Examples**

This example shows how to disable the STP on VLAN 5:

```
Switch(config)# no spanning-tree vlan 5
```

You can verify your setting by entering the **show spanning-tree** privileged EXEC command. In this instance, VLAN 5 does not appear in the list.

This example shows how to set the spanning-tree forwarding time to 18 seconds for VLANs 20 and 25:

```
Switch(config)# spanning-tree vlan 20,25 forward-time 18
```

This example shows how to set the spanning-tree hello-delay time to 3 seconds for VLANs 20 to 24:

```
Switch(config)# spanning-tree vlan 20-24 hello-time 3
```

This example shows how to set spanning-tree max-age to 30 seconds for VLAN 20:

```
Switch(config)# spanning-tree vlan 20 max-age 30
```

This example shows how to reset the **max-age** parameter to the default value for spanning-tree instance 100 and 105 to 108:

```
Switch(config)# no spanning-tree vlan 100, 105-108 max-age
```

This example shows how to set the spanning-tree priority to 8192 for VLAN 20:

```
Switch(config)# spanning-tree vlan 20 priority 8192
```

This example shows how to configure the switch as the root switch for VLAN 10 with a network diameter of 4:

```
Switch(config)# spanning-tree vlan 10 root primary diameter 4
```

This example shows how to configure the switch as the secondary root switch for VLAN 10 with a network diameter of 4:

```
Switch(config)# spanning-tree vlan 10 root secondary diameter 4
```

You can verify your settings by entering the **show spanning-tree vlan *vlan-id*** privileged EXEC command.

#### Related Commands

Command	Description
<a href="#">show spanning-tree vlan</a>	Displays spanning-tree information.
<a href="#">spanning-tree cost</a>	Sets the path cost for spanning-tree calculations.
<a href="#">spanning-tree guard</a>	Enables the root guard or the loop guard feature for all the VLANs associated with the selected interface.
<a href="#">spanning-tree port-priority</a>	Sets an interface priority.
<a href="#">spanning-tree portfast (global configuration)</a>	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled STP ports or enables the Port Fast feature on all nontrunking STP ports.
<a href="#">spanning-tree portfast (interface configuration)</a>	Enables the Port Fast feature on an STP port in all its associated VLANs.

# speed

Use the **speed** interface configuration command to specify the speed of a 10/100 Mbps or 10/100/1000 Mbps port. Use the **no** or **default** form of this command to return the port to its default value.

```
speed {10 | 100 | 1000 | auto [10 | 100 | 1000] | nonegotiate}
```

```
no speed
```



## Note

For speed configurations restrictions on small form-factor pluggable (SFP) module ports, see the “Usage Guidelines” section.



## Note

You cannot configure the speed on small form-factor pluggable (SFP) module ports, but you can configure the speed to not negotiate (**nonegotiate**) if they are connected to a device that does not support autonegotiation. See “Usage Guidelines” for exceptions when a 1000BASE-T SFP module is in the SFP module slot.

## Syntax Description

<b>10</b>	Port runs at 10 Mbps.
<b>100</b>	Port runs at 100 Mbps.
<b>1000</b>	Port runs at 1000 Mbps. This option is valid and visible only on 10/100/1000 Mbps-ports.
<b>auto</b>	Port automatically detects the speed it should run at based on the port at the other end of the link. If you use the <b>10</b> , <b>100</b> , or <b>1000</b> keywords with the <b>auto</b> keyword, the port only autonegotiates at the specified speeds.
<b>nonegotiate</b>	Autonegotiation is disabled, and the port runs at 1000 Mbps. (The 1000BASE-T SFP does not support the <b>nonegotiate</b> keyword.)

## Defaults

The default is **auto**.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

You can configure the Fast Ethernet port speed as either 10 or 100 Mbps.

You can configure the Gigabit Ethernet port speed as 10, 100, or 1000 Mbps.

When a 1000BASE-T SFP module is in the SFP module slot, you can configure the speed as **10**, **100**, **1000**, or **auto** but not to **nonegotiate**.

Except for the 1000BASE-T SFP modules, if an SFP module port is connected to a device that does not support autonegotiation, you can configure the speed to not negotiate (**nonegotiate**).

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

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

**Caution**

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

**Note**

For guidelines on setting the switch speed and duplex parameters, see the software configuration guide for this release.

**Examples**

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

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed 100
```

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

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed auto 10
```

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

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed auto 10 100
```

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

**Related Commands**

Command	Description
<a href="#">duplex</a>	Specifies the duplex mode of operation.
<a href="#">show interfaces</a>	Displays the statistical information specific to all interfaces or to a specific interface.

## storm-control

Use the **storm-control** interface configuration command to enable broadcast, multicast, or unicast storm control and to set threshold levels on an interface. Use the **no** form of this command to return to the default setting.

```
storm-control {{broadcast | multicast | unicast} level {level [level-low] | bps bps [bps-low] | pps pps [pps-low]}} | {action {shutdown | trap}}
```

```
no storm-control {{broadcast | multicast | unicast} level} | {action {shutdown | trap}}
```

### Syntax Description

<b>broadcast</b>	Enable broadcast storm control on the interface.
<b>multicast</b>	Enable multicast storm control on the interface.
<b>unicast</b>	Enable unicast storm control on the interface.
<b>level</b> <i>level</i> [ <i>level-low</i> ]	Specify the rising and falling suppression levels as a percentage of total bandwidth of the port. <ul style="list-style-type: none"> <li><i>level</i>—Rising suppression level, up to two decimal places. The range is 0.00 to 100.00. Block the flooding of storm packets when the value specified for <i>level</i> is reached.</li> <li><i>level-low</i>—(Optional) Falling suppression level, up to two decimal places. The range is 0.00 to 100.00. This value must be less than or equal to the rising suppression value. If you do not configure a falling suppression level, it is set to the rising suppression level.</li> </ul>
<b>level</b> <b>bps</b> <i>bps</i> [ <i>bps-low</i> ]	Specify the rising and falling suppression levels as a rate in bits per second at which traffic is received on the port. <ul style="list-style-type: none"> <li><i>bps</i>—Rising suppression level, up to 1 decimal place. The range is 0.0 to 10000000000.0. Block the flooding of storm packets when the value specified for <i>bps</i> is reached.</li> <li><i>bps-low</i>—(Optional) Falling suppression level, up to 1 decimal place. The range is 0.0 to 10000000000.0. This value must be equal to or less than the rising suppression value.</li> </ul> <p>You can use metric suffixes such as k, m, and g for large number thresholds.</p>



<b>level</b> <i>pps pps</i> [ <i>pps-low</i> ]	Specify the rising and falling suppression levels as a rate in packets per second at which traffic is received on the port. <ul style="list-style-type: none"> <li><i>pps</i>—Rising suppression level, up to 1 decimal place. The range is 0.0 to 10000000000.0. Block the flooding of storm packets when the value specified for <i>pps</i> is reached.</li> <li><i>pps-low</i>—(Optional) Falling suppression level, up to 1 decimal place. The range is 0.0 to 10000000000.0. This value must be equal to or less than the rising suppression value.</li> </ul> <p>You can use metric suffixes such as k, m, and g for large number thresholds.</p>
<b>action</b> { <b>shutdown</b>   <b>trap</b> }	Action taken when a storm occurs on a port. The default action is to filter traffic and to not send an Simple Network Management Protocol (SNMP) trap. <p>The keywords have these meanings:</p> <ul style="list-style-type: none"> <li><b>shutdown</b>—Disables the port during a storm.</li> <li><b>trap</b>—Sends an SNMP trap when a storm occurs.</li> </ul>

**Defaults**

Broadcast, multicast, and unicast storm control are disabled.  
The default action is to filter traffic and to not send an SNMP trap.

**Command Modes**

Interface configuration

**Command History**

Release	Modification
12.2(44)EY	This command was introduced.

**Usage Guidelines**

Storm control is supported on physical interfaces. You can also configure storm control on an EtherChannel. When storm control is configured on an EtherChannel, the storm control settings propagate to the EtherChannel physical interfaces.

If the port is a user network interface (UNI) or enhanced network interfaces (ENI), you must use the **no shutdown** interface configuration command to enable it before using the **storm-control** command. UNIs and ENIs are disabled by default. Network node interfaces (NNIs) are enabled by default.

The storm-control suppression level can be entered as a percentage of total bandwidth of the port, as a rate in packets per second at which traffic is received, or as a rate in bits per second at which traffic is received.

When specified as a percentage of total bandwidth, a suppression value of 100 percent means that no limit is placed on the specified traffic type. A value of **level 0 0** means that all broadcast, multicast, or unicast traffic on that port is blocked. Storm control is enabled only when the rising suppression level is less than 100 percent. If no other storm-control configuration is specified, the default action is to filter the traffic causing the storm and to send no SNMP traps.

**Note**

When the storm control threshold for multicast traffic is reached, all multicast traffic except control traffic, such as bridge protocol data unit (BDPU) and Cisco Discovery Protocol (CDP) frames, are blocked. However, the switch does not differentiate between routing updates, such as Open Shortest Path First (OSPF) and regular multicast data traffic, so both types of traffic are blocked.

The **trap** and **shutdown** options are independent of each other.

If you configure the action to be taken as shutdown (the port is error-disabled during a storm) when a packet storm is detected, you must use the **no shutdown** interface configuration command to bring the interface out of this state. If you do not specify the **shutdown** action, specify the action as **trap** (the switch generates a trap when a storm is detected).

When a storm occurs and the action is to filter traffic, if the falling suppression level is not specified, the switch blocks all traffic until the traffic rate drops below the rising suppression level. If the falling suppression level is specified, the switch blocks traffic until the traffic rate drops below this level.

When a broadcast storm occurs and the action is to filter traffic, the switch blocks only broadcast traffic.

For more information, see the software configuration guide for this release.

**Examples**

This example shows how to enable broadcast storm control with a 75.5-percent rising suppression level:

```
Switch(config-if)# storm-control broadcast level 75.5
```

This example shows how to enable unicast storm control on a port with a 87-percent rising suppression level and a 65-percent falling suppression level:

```
Switch(config-if)# storm-control unicast level 87 65
```

This example shows how to enable multicast storm control on a port with a 2000-packets-per-second rising suppression level and a 1000-packets-per-second falling suppression level:

```
Switch(config-if)# storm-control multicast level pps 2k 1k
```

This example shows how to enable the **shutdown** action on a port:

```
Switch(config-if)# storm-control action shutdown
```

You can verify your settings by entering the **show storm-control** privileged EXEC command.

**Related Commands**

Command	Description
<a href="#">show storm-control</a>	Displays broadcast, multicast, or unicast storm control settings on all interfaces or on a specified interface.

# switchport

Use the **switchport** interface configuration command with no keywords to put an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration. Use the **no** form of this command to put an interface in Layer 3 mode.

**switchport**

**no switchport**

## Syntax Description

This command has no arguments or keywords.

## Defaults

By default, all interfaces are in Layer 2 (switching) mode.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

Use the **no switchport** command (without parameters) to set the interface to the routed-interface status and to erase all Layer 2 configurations. You must enter the **no switchport** command and then assign an IP address to the port.

If an interface is configured you must first enter the **switchport** command with no keywords before configuring switching characteristics on the port. Then you can enter additional **switchport** commands with keywords, as shown on the pages that follow.

Entering the **no switchport** command shuts the port down and then re-enables it, which might generate messages on the device to which the port is connected.

When you enter the **switchport** (or **no switchport**) command without keywords on an interface, the configuration information for the affected interface might be lost, and the interface returned to its default configuration.

## Examples

This example shows how to change an interface from a Layer 2 (switching) port to a Layer 3 (routed) port.

```
Switch(config-if)# no switchport
```

This example shows how to return the port to switching mode:

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

You can verify the switchport status of an interface by entering the **show running-config** privileged EXEC command.

Related Commands	Command	Description
	<b>show interfaces switchport</b>	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
	<b>show running-config</b>	Displays the operating configuration.

# switchport access vlan

Use the **switchport access vlan** interface configuration command to configure a port as a static-access or dynamic-access port. If the switchport mode is set to **access** (by using the **switchport mode** interface configuration command), use this command to set the port to operate as a member of the specified VLAN or to specify that the port uses VLAN Membership Policy Server (VMPS) protocol where VLAN assignment based on the incoming packets it receives. Use the **no** form of this command to reset the access VLAN mode to the default VLAN for the switch.

**switchport access vlan** {*vlan-id* | **dynamic**}

**no switchport access vlan**

Syntax Description		
	<i>vlan-id</i>	Configure the interface as a static access port with the VLAN ID of the access mode VLAN; the range is 1 to 4094.
	<b>dynamic</b>	Specify that the access mode VLAN is dependent on the VMPS protocol. The port is assigned to a VLAN based on the source MAC address of a host (or hosts) connected to the port. The switch sends every new MAC address received to the VMPS server to obtain the VLAN name to which the dynamic-access port should be assigned. If the port already has a VLAN assigned and the source has already been approved by the VMPS, the switch forwards the packet to the VLAN.
	<b>Note</b>	This keyword is visible only on user network interfaces (UNIs) or enhanced network interfaces (ENIs).

Defaults	
	The default access VLAN and trunk interface native VLAN is a 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

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

Usage Guidelines	
	The <b>no switchport access vlan</b> command resets the access mode VLAN to the appropriate default VLAN for the device.
	The port must be in access mode before the <b>switchport access vlan</b> command can take effect.
	An access port can be assigned to only one VLAN.
	The VMPS server (such as a Catalyst 6500 series switch) must be configured before a port is configured as dynamic.

If the specified VLAN is configured as a UNI-ENI community VLAN, the interface is configured as UNI-ENI community port. Otherwise the port is configured as a UNI-ENI isolated port.

This command is supported on IEEE802.1Q tunnel ports.

These restrictions apply to dynamic-access ports:

- The **dynamic** keyword is not visible on network node interfaces (NNIs).
- The software implements the VLAN Query Protocol (VQP) client, which can query a VMPS such as a Catalyst 6500 series switch. The switch cannot be a VMPS servers. The VMPS server must be configured before a port is configured as dynamic.
- Use dynamic-access ports only to connect end stations. Connecting them to switches or routers (that use bridging protocols) can cause a loss of connectivity.
- Dynamic-access ports can only be in one VLAN and do not use VLAN tagging.
- Dynamic-access ports cannot be configured as:
  - Members of an EtherChannel port group (dynamic-access ports cannot be grouped with any other port, including other dynamic ports).
  - Source or destination ports in a static address entry.
  - Monitor ports.

### Examples

This example shows how to change a Layer 2 interface in access mode to operate in VLAN 2 instead of the default VLAN.

```
Switch(config-if)# switchport access vlan 2
```

You can verify your setting by entering the **show interfaces interface-id switchport** privileged EXEC command and examining information in the Administrative Mode and Operational Mode rows.

### Related Commands

Command	Description
<b>show interfaces switchport</b>	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
<b>switchport mode</b>	Configures the VLAN membership mode of a port.

# switchport backup interface

Use the **switchport backup interface** interface configuration command on a Layer 2 interface on the switch stack or on a standalone switch to configure Flex Links, a pair of interfaces that provide backup to each other. Use the **no** form of this command to remove the Flex Links configuration.

```
switchport backup interface [FastEthernet interface-id | GigabitEthernet interface-id |
Port-channel interface-id] {mmu primary vlan interface-id | multicast fast-convergence |
preemption {delay delay-time | mode} | prefer vlan vlan-id}
```

```
no switchport backup interface [FastEthernet interface-id | GigabitEthernet interface-id |
Port-channel interface-id] {mmu primary vlan interface-id | multicast fast-convergence |
preemption {delay delay-time | mode} | prefer vlan vlan-id}
```

Syntax	Description
<b>FastEthernet</b>	FastEthernet IEEE 802.3 port name. Valid range is 0 to 9.
<b>GigabitEthernet</b>	GigabitEthernet IEEE 802.3z port name. Valid range is 0 to 9.
<b>Port-channel</b>	Ethernet Channel of interface. Valid range is 0 to 48.
<i>interface-id</i>	Specify that the Layer 2 interface to act as a backup link to the interface being configured. The interface can be a physical interface or port channel. The port-channel range is 1 to 486.
<b>mmu</b>	MAC-address move update. Configure the MAC move update (MMU) for a backup interface pair.
<b>primary vlan</b> <i>vlan-id</i>	The VLAN ID of the private-VLAN primary VLAN; valid range is 1 to 4,094.
<b>multicast fast-convergence</b>	Multicast Fast-convergence parameter.
<b>preemption</b>	Configure a preemption scheme for a backup interface pair.
<b>delay</b> <i>delay-time</i>	(Optional) Specify a preemption delay; the valid values are 1 to 300 seconds.
<b>mode</b>	Specify a preemption mode as bandwidth, forced, or off.
<b>prefer vlan</b> <i>vlan-id</i>	Specify that VLANs are carried on the backup interfaces of a Flex Link pair. VLAN ID range is 1 to 4,094.
<b>off</b>	(Optional) Specify that no preemption occurs from backup to active.
<b>delay</b> <i>delay-time</i>	(Optional) Specify a preemption delay; the valid values are 1 to 300 seconds.

## Defaults

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

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

**Usage Guidelines**

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.

**Examples**

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

```
Switch# configure terminal
Switch(conf)# interface fastethernet0/1
Switch(conf-if)# switchport backup interface fastethernet0/2
Switch(conf-if)# end
```

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

```
Switch# configure terminal
Switch(conf)# interface fastethernet0/1
Switch(conf-if)# switchport backup interface fastethernet0/2 preemption forced
Switch(conf-if)# end
```

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

```
Switch# configure terminal
Switch(conf)# interface fastethernet0/1
Switch(conf-if)# switchport backup interface fastethernet0/2 preemption delay 150
Switch(conf-if)# end
```

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

```
Switch# configure terminal
Switch(conf)# interface fastethernet0/1
Switch(conf-if)# switchport backup interface fastethernet0/2 mmu primary vlan 1021
Switch(conf-if)# end
```

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

The following example shows how to configure preferred VLANs:

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



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

In the following example, VLANs 60, and 100 to 120 are configured on the switch:

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

When both interfaces are up, Gi0/6 forwards traffic for VLANs 1 to 50, and Gi0/8 forwards traffic for VLANs 60 and 100 to 120.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
GigabitEthernet0/6	GigabitEthernet0/8	Active Up/Backup Up

```
Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 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 Gi0/6 goes down, Gi0/8 carries all VLANs of the Flex Link pair.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
GigabitEthernet0/6	GigabitEthernet0/8	Active Down/Backup Up

```
Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 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 Gi0/6 comes up, VLANs preferred on this interface are blocked on the peer interface Gi0/8 and forwarded on Gi0/6.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
GigabitEthernet0/6	GigabitEthernet0/8	Active Up/Backup Up

```
Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

The following example shows how to configure multicast fast-convergence on interface Gi0/11:

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet 0/11
Switch(config-if)# switchport backup interface gigabitEthernet 0/12 multicast
fast-convergence
Switch(config-if)# end
```

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

```
Switch# show interfaces switchport backup detail
```

```
Switch Backup Interface Pairs:
```

```
Active Interface      Backup Interface      State
-----
GigabitEthernet0/11  GigabitEthernet0/12  Active Up/Backup Standby
Preemption Mode      : off
Multicast Fast Convergence : On
Bandwidth : 1000000 Kbit (Gi0/11), 1000000 Kbit (Gi0/12)
Mac Address Move Update Vlan : auto
```

#### Related Commands

Command	Description
<a href="#">show interfaces</a> [ <i>interface-id</i> ] <b>switchport backup</b>	Displays the configured Flex Links and their status on the switch or for the specified interface.

# switchport block

Use the **switchport block** interface configuration command to prevent unknown multicast or unicast packets from being forwarded. Use the **no** form of this command to allow forwarding unknown multicast or unicast packets.

**switchport block** {multicast | unicast}

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

## Syntax Description

<b>multicast</b>	Specify that unknown multicast traffic should be blocked. <b>Note</b> Only pure Layer 2 multicast traffic is blocked. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.
<b>unicast</b>	Specify that unknown unicast traffic should be blocked.

## Defaults

Unknown multicast and unicast traffic is not blocked.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

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.

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.

If the port is a user network interface (UNI) or enhanced network interface (ENI), you must use the **no shutdown** interface configuration command to enable it before using the **switchport block** command. UNIs and ENIs are disabled by default. Network node interfaces (NNIs) are enabled by default.

Blocking unknown multicast or unicast traffic is not automatically enabled on protected ports; you must explicitly configure it.



### Note

For more information about blocking packets, see the software configuration guide for this release.

## Examples

This example shows how to block unknown multicast traffic on an interface:

```
Switch(config-if)# switchport block multicast
```

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

## ■ switchport block

Related Commands	Command	Description
	<a href="#">show interfaces switchport</a>	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.

# switchport host

Use the **switchport host** interface configuration command to optimize a Layer 2 port for a host connection. The **no** form of this command has no effect on the system.

## switchport host

### Syntax Description

This command has no arguments or keywords.

### Defaults

The default is for the port to not be optimized for a host connection.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

To optimize the port for a host connection, the **switchport host** command sets switch port mode to access, enables spanning tree Port Fast, and disables channel grouping. Only an end station can accept this configuration.

Because spanning tree Port Fast is enabled, you should enter the **switchport host** command only on ports that are connected to a single host. Connecting other switches, hubs, concentrators, or bridges to a fast-start port can cause temporary spanning-tree loops.

Enable the **switchport host** command to decrease the time that it takes to start up packet forwarding.

### Examples

This example shows how to optimize the port configuration for a host connection:

```
Switch(config-if)# switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
Switch(config-if)#
```

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

### Related Commands

Command	Description
<b>show interfaces <i>switchport</i></b>	Displays the administrative and operational status of a switching (nonrouting) port, including switchport mode.

# switchport mode

Use the **switchport mode** interface configuration command to configure the VLAN membership mode of a port. Use the **no** form of this command to reset the mode to the default.

**switchport mode** { **access** | **dot1q-tunnel** | **private-vlan** | **trunk** }

**no switchport mode**

## Syntax Description

<b>access</b>	Set the port to access mode (either static-access or dynamic-access depending on the setting of the <b>switchport access vlan</b> interface configuration command). The port is set to access unconditionally and operates as a nontrunking, single VLAN interface that sends and receives unencapsulated (nontagged) frames. An access port can be assigned to only one VLAN.
<b>dot1q-tunnel</b>	Set the port as an IEEE 802.1Q tunnel port. This keyword is supported only when the metro IP access or metro access image is running on the switch.
<b>private-vlan</b>	See the <a href="#">switchport mode private-vlan</a> command.
<b>trunk</b>	Set the port to trunk unconditionally. The port is a trunking VLAN Layer 2 interface. The port sends and receives encapsulated (tagged) frames that identify the VLAN of origination. A trunk is a point-to-point link between two switches or between a switch and a router.

## Defaults

The default mode is **access**.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

A configuration that uses the **access**, **dot1q-tunnel**, 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. If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.

When you enter **dot1q-tunnel**, the port is set unconditionally as an IEEE 802.1Q tunnel port.

Access ports, and trunk ports, and tunnel ports are mutually exclusive.

Any IEEE 802.1Q encapsulated IP packets received on a tunnel port can be filtered by MAC access control lists (ACLs), but not by IP ACLs. This is because the switch does not recognize the protocol inside the IEEE 802.1Q header. This restriction applies to router ACLs, port ACLs, and VLAN maps.

Configuring a port as an 802.1Q tunnel port has these limitations:

- IP routing is not supported on tunnel ports.
- Tunnel ports do not support IP ACLs.
- If an IP ACL is applied to a trunk port in a VLAN that includes tunnel ports, or if a VLAN map is applied to a VLAN that includes tunnel ports, packets received from the tunnel port are treated as non-IP packets and are filtered with MAC access lists.
- Layer 3 quality of service (QoS) ACLs and other QoS features related to Layer 3 information are not supported on tunnel ports.


**Note**

For more information about configuring IEEE 802.1Q tunnel ports, see the software configuration guide for this release.

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 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.


**Note**

Only user network interfaces (UNIs) or enhanced network interfaces (ENIs) can be dynamic-access ports.

**Examples**

This example shows how to configure a port for access mode:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode access
```

This example shows how to configure a port for trunk mode:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode trunk
```

This example shows how to configure a port as an IEEE 802.1Q tunnel port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode dot1q-tunnel
```

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.

## ■ switchport mode

Related Commands	Command	Description
	<a href="#">show interfaces switchport</a>	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
	<a href="#">switchport access vlan</a>	Configures a port as a static-access or dynamic-access port.
	<a href="#">switchport trunk</a>	Configures the trunk characteristics when an interface is in trunking mode.



# switchport mode private-vlan

Use the **switchport mode private-vlan** interface configuration command to configure a port as a promiscuous or host private VLAN port. Use the **no switchport mode** command to reset the mode to the default access mode.

```
switchport mode private-vlan {host | promiscuous}
```

```
no switchport mode private-vlan
```



## Note

The **promiscuous** keyword is visible only on network node interfaces (NNIs).

## Syntax Description

<b>host</b>	Configure the interface as a private-VLAN host port. Host ports belong to private-VLAN secondary VLANs and are either community ports or isolated ports, depending on the VLAN that they belong to.
<b>promiscuous</b>	Configure the interface as a private-VLAN promiscuous port. Promiscuous ports are members of private-VLAN primary VLANs. This keyword is only available on NNIs. User network interfaces (UNIs) or enhanced network interfaces (ENIs) cannot be configured as private VLAN promiscuous ports.

## Defaults

The default private-VLAN mode is neither host nor promiscuous.  
The default switchport mode is **access**.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

A private-VLAN promiscuous port must be an NNI. To configure a UNI or an ENI as an NNI, enter the **port-type nni** interface configuration command.

A private-VLAN host or promiscuous port cannot be a Switched Port Analyzer (SPAN) destination port. If you configure a SPAN destination port as a private-VLAN host or promiscuous port, the port becomes inactive.

Do not configure private VLAN on ports with these other features:

- dynamic-access port VLAN membership
- Port Aggregation Protocol (PAgP) for only NNIs or ENIs
- Link Aggregation Control Protocol (LACP) only for NNIs or ENIs
- Multicast VLAN Registration (MVR)

A private-VLAN port cannot be a SPAN destination port.

While a port is part of the private-VLAN configuration, any EtherChannel configuration for it is inactive. A private-VLAN port cannot be a secure port and should not be configured as a protected port.

**Note**

For more information about private-VLAN interaction with other features, see the software configuration guide for this release.

If the port has STP enabled, we strongly recommend that you enable spanning tree Port Fast and bridge-protocol-data-unit (BPDU) guard on isolated and community host ports to prevent STP loops due to misconfigurations and to speed up STP convergence.

If you configure a port as a private-VLAN host port and you do not configure a valid private-VLAN association by using the **switchport private-vlan host-association** interface configuration command, the interface becomes inactive.

If you configure an NNI as a private-VLAN promiscuous port and you do not configure a valid private VLAN mapping by using the **switchport private-vlan mapping** interface configuration command, the interface becomes inactive.

**Examples**

This example shows how to configure an interface as a private-VLAN host port and associate it to primary VLAN 20. The interface is a member of secondary isolated VLAN 501 and primary VLAN 20.

**Note**

When you configure an NNI as a private VLAN host port, you should also enable BPDU guard and Port Fast by using the **spanning-tree portfast bpduguard default** global configuration command and the **spanning-tree portfast** interface configuration command.

```
Switch# configure terminal
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 20 501
Switch(config-if)# end
```

This example shows how to configure an NNI as a private VLAN promiscuous port and map it to a private VLAN. The interface is a member of primary VLAN 20 and secondary VLANs 501 to 503 are mapped to it.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 501-503
Switch(config-if)# end
```

You can verify private VLAN switchport mode by using the **show interfaces interface-id switchport** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">private-vlan</a>	Configures a VLAN as a community, isolated, or primary VLAN or associates a primary VLAN with secondary VLANs.
	<a href="#">show interfaces switchport</a>	Displays the administrative and operational status of a switching (nonrouting) port, including private VLAN configuration.
	<a href="#">switchport private-vlan</a>	Configures private VLAN associations and mappings between primary and secondary VLANs on an interface.

## switchport port-security

Use the **switchport port-security** interface configuration command without keywords to enable port security on the interface. Use the keywords to configure secure MAC addresses, sticky MAC address learning, a maximum number of secure MAC addresses, or the violation mode. Use the **no** form of this command to disable port security or to set the parameters to their default states.

```
switchport port-security [mac-address mac-address [vlan access] | mac-address sticky
[mac-address | vlan access]] [maximum value [vlan access]]
```

```
no switchport port-security [mac-address mac-address [vlan access] | mac-address sticky
[mac-address | vlan access]] [maximum value [vlan access]]
```

```
switchport port-security [aging] [violation {protect | restrict | shutdown}]
```

```
no switchport port-security [aging] [violation {protect | restrict | shutdown}]
```

Syntax Description	
<b>aging</b>	(Optional) See the <a href="#">switchport port-security aging</a> command.
<b>mac-address</b> <i>mac-address</i>	(Optional) Specify 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.
<b>vlan</b> <i>vlan-id</i>	(Optional) On a trunk port only, specify the VLAN ID and the MAC address. If no VLAN ID is specified, the native VLAN is used.
<b>vlan access</b>	(Optional) On an access port only, specify the VLAN as an access VLAN.
<b>mac-address sticky</b> <i>[mac-address]</i>	(Optional) Enable the interface for <i>sticky learning</i> by entering only the <b>mac-address sticky</b> keywords. 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.  (Optional) Enter a <i>mac-address</i> to specify a sticky secure MAC address.
<b>maximum</b> <i>value</i>	(Optional) Set the maximum number of secure MAC addresses for the interface. The maximum number of secure MAC addresses that you can configure on a switch 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 <a href="#">sdm prefer</a> 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.  The default setting is 1.
<b>vlan</b> [ <i>vlan-list</i> ]	(Optional) For trunk ports, you can set the maximum number of secure MAC addresses on a VLAN. If the <b>vlan</b> keyword is not entered, the default value is used. <ul style="list-style-type: none"> <li><b>vlan</b>—set a per-VLAN maximum value.</li> <li><b>vlan</b> <i>vlan-list</i>—set a per-VLAN maximum value on a 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.</li> </ul>

<b>violation</b>	(Optional) Set the security violation mode or the action to be taken if port security is violated. The default is <b>shutdown</b> .
<b>protect</b>	Set the security violation protect mode. In this 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.  <b>Note</b> 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.
<b>restrict</b>	Set the security violation restrict mode. In this 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.
<b>shutdown</b>	Set the security violation shutdown mode. In this 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 <b>errdisable recovery cause psecure-violation</b> global configuration command, or you can manually re-enable it by entering the <b>shutdown</b> and <b>no shut down</b> interface configuration commands.

**Defaults**

The default is to disable port security.

When port security is enabled and no keywords are entered, the default maximum number of secure MAC addresses is 1.

The default violation mode is **shutdown**.

Sticky learning is disabled.

**Command Modes**

Interface configuration

**Command History**

Release	Modification
12.2(44)EY	This command was introduced.

**Usage Guidelines**

If the port is a user network interface (UNI) or enhanced network interface (ENI), you must use the **no shutdown** interface configuration command to enable it before using the **switchport port-security** command. UNIs and ENIs are disabled by default. Network node interfaces (NNIs) are enabled by default.

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 Fast EtherChannel or Gigabit EtherChannel port group.
- 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.
- The switch does not support port security aging of sticky secure MAC addresses.

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, or you can manually re-enable it by entering the **shutdown** and **no shut down** interface configuration commands.

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.

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.

### Examples

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.

```
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
```

This example shows how to configure a secure MAC address and a VLAN ID on a port.

```
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(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:

```
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.4141
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.000f
```

You can verify your settings by using the **show port-security** privileged EXEC command.

### Related Commands

Command	Description
<b>clear port-security</b>	Deletes from the MAC address table a specific type of secure address or all the secure addresses on the switch or an interface.
<b>show port-security address</b>	Displays all the secure addresses configured on the switch.
<b>show port-security interface interface-id</b>	Displays port security configuration for the switch or for the specified interface.

## switchport port-security aging

Use the **switchport port-security aging** interface configuration command 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 **no** form of this command to disable port security aging or to set the parameters to their default states.

```
switchport port-security aging {static | time time | type {absolute | inactivity}}
```

```
no switchport port-security aging {static | time | type}
```

### Syntax Description

<b>static</b>	Enable aging for statically configured secure addresses on this port.
<b>time</b> <i>time</i>	Specify the aging time for this port. The range is 0 to 1440 minutes. If the time is 0, aging is disabled for this port.
<b>type</b>	Set the aging type.
<b>absolute</b>	Set 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.
<b>inactivity</b>	Set 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.

### Defaults

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
12.2(44)EY	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. If the port is a user network interface (UNI) or enhanced network interface (ENI), you must use the **no shutdown** interface configuration command to enable it before using the **switchport port-security aging** command. UNIs and ENIs are disabled by default. Network node interfaces (NNIs) are enabled by default.

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.



**Examples**

This example sets the aging time as 2 hours for absolute aging for all the secure addresses on the port.

```
Switch(config)# interface gigabitethernet0/1
Switch(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.

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport port-security aging time 2
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static
```

This example shows how to disable aging for configured secure addresses.

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no switchport port-security aging static
```

**Related Commands**

Command	Description
<a href="#">show port-security</a>	Displays the port security settings defined for the port.
<a href="#">switchport port-security</a>	Enables port security on a port, restricts the use of the port to a user-defined group of stations, and configures secure MAC addresses.

# switchport private-vlan

Use the **switchport private-vlan** interface configuration command to define a private-VLAN association for an isolated or community port or a mapping for a promiscuous port. Use the **no** form of this command to remove the private-VLAN association or mapping from the port.

```
switchport private-vlan { association { host primary-vlan-id secondary-vlan-id | mapping
primary-vlan-id { add | remove } secondary-vlan-list } | host-association primary-vlan-id
secondary-vlan-id | mapping primary-vlan-id { add | remove } secondary-vlan-list }
```

```
no switchport private-vlan { association { host | mapping } | host-association | mapping }
```



## Note

The mapping commands are supported only on network node interfaces (NNIs).

## Syntax Description

<b>association</b>	Define a private-VLAN association for a port.
<b>host</b>	Define a private-VLAN association for a community or isolated host port.
<i>primary-vlan-id</i>	The VLAN ID of the private-VLAN primary VLAN. The range is from 2 to 1001 and 1006 to 4094.
<i>secondary-vlan-id</i>	The VLAN ID of the private-VLAN secondary (isolated or community) VLAN. The range is from 2 to 1001 and 1006 to 4094.
<b>mapping</b>	Define private-VLAN mapping for a promiscuous port. Only NNIs can be configured as promiscuous ports. This keyword is not supported on user network interfaces (UNIs) or enhanced network interfaces (ENIs).
<b>add</b>	Associate secondary VLANs to the primary VLAN.
<b>remove</b>	Clear the association between secondary VLANs and the primary VLAN.
<i>secondary-vlan-list</i>	One or more secondary (isolated or community) VLANs to be mapped to the primary VLAN.
<b>host-association</b>	Define a private-VLAN association for a community or isolated host port.

## Defaults

The default is to have no private-VLAN association or mapping configured.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

Private-VLAN association or mapping has no effect on the port unless the port has been configured as a private-VLAN host or promiscuous port by using the **switchport mode private-vlan** { **host** | **promiscuous** } interface configuration command.

A promiscuous port must be an NNI; UNIs or ENIs cannot be configured as promiscuous ports. To configure a port as a UNI, enter the **port-type uni** interface configuration command.

If the port is in private-VLAN host or promiscuous mode but the VLANs do not exist, the command is allowed, but the port is made inactive.

The *secondary\_vlan\_list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private-VLAN ID or a hyphenated range of private-VLAN IDs. The list can contain one isolated VLAN and multiple community VLANs.

You can map a promiscuous port to only one primary VLAN. If you enter the **switchport private-vlan mapping** command on a promiscuous port that is already mapped to a primary and secondary VLAN, the primary VLAN mapping is overwritten.

You can add or remove secondary VLANs from promiscuous port private-VLAN mappings by using the **add** and **remove** keywords.

Entering the **switchport private-vlan association host** command has the same effect as entering the **switchport private-vlan host-association** interface configuration command.

Entering the **switchport private-vlan association mapping** command has the same effect as entering the **switchport private-vlan mapping** interface configuration command.

## Examples

This example shows how to configure an interface as a private VLAN host port and associate it with primary VLAN 20 and secondary VLAN 501:

```
Switch# configure terminal
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 20 501
Switch(config-if)# end
```

This example shows how to configure an NNI as a private-VLAN promiscuous port and map it to a private VLAN. The interface is a member of primary VLAN 20 and secondary VLANs 501 to 503 are mapped to it.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 add 501-503
Switch(config-if)# end
```

You can verify private-VLAN mapping by using the **show interfaces private-vlan mapping** privileged EXEC command.

## Related Commands

Command	Description
<b>show interfaces private-vlan mapping</b>	Displays private VLAN mapping information for <b>VLAN SVIs</b> .?
<b>show vlan private-vlan</b>	Displays all private VLAN relationships or types configured on the switch.

# switchport protected

Use the **switchport protected** interface configuration command to isolate unicast, multicast, and broadcast traffic at Layer 2 from other protected ports on the same switch. Use the **no** form of this command to disable protection on the port.

**switchport protected**

**no switchport protected**



## Note

Protected ports are supported only on network node interfaces (NNIs).

## Syntax Description

This command has no arguments or keywords.

## Defaults

No protected port is defined. All ports are nonprotected.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The switchport protection feature is local to the switch; communication between protected ports on the same switch is possible only through a Layer 3 device. To prevent communication between protected ports on different switches, you must configure the protected ports for unique VLANs on each switch and configure a trunk link between the switches. A protected port is different from a secure port.

A protected port does not forward any traffic (unicast, multicast, or broadcast) to any other port that is also a protected port. Data traffic cannot be forwarded between protected ports at Layer 2; only control traffic, such as PIM packets, is forwarded because these packets are processed by the CPU and forwarded in software. All data traffic passing between protected ports must be forwarded through a Layer 3 device.

Port monitoring does not work if both the monitor and monitored ports are protected ports.

## Examples

This example shows how to enable a protected port on an interface:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport protected
```

You can verify your settings by entering the **show interfaces interface-id switchport** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">show interfaces switchport</a>	Displays the administrative and operational status of a switching port, including port blocking and port protection settings.
	<a href="#">switchport block</a>	Prevents unknown multicast or unicast traffic on the interface.

# switchport trunk

Use the **switchport trunk** interface configuration command to set the trunk characteristics when the interface is in trunking mode. Use the **no** form of this command to reset a trunking characteristic to the default.

**switchport trunk** { **allowed vlan** *vlan-list* | **native vlan** *vlan-id* }

**no switchport trunk** { **allowed vlan** | **native vlan** }

## Syntax Description

<b>allowed vlan</b> <i>vlan-list</i>	Set the list of allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode. See the following <i>vlan-list</i> format. The <b>none</b> keyword is not valid. The default is <b>all</b> .
<b>native vlan</b> <i>vlan-id</i>	Set the native VLAN for sending and receiving untagged traffic when the interface is in 802.1Q trunking mode. The range is 1 to 4094.

The *vlan-list* format is **all** | **none** | [**add** | **remove** | **except**] *vlan-atom* [, *vlan-atom*...] where:

- **all** specifies all VLANs from 1 to 4094. This keyword is not allowed on commands that do not permit all VLANs in the list to be set at the same time.
- **none** means an empty list. This keyword is not allowed on commands that require certain VLANs to be set or at least one VLAN to be set.
- **add** adds the defined list of VLANs to those currently set instead of replacing the list. Valid IDs are from 1 to 4094. You can add extended-range VLANs (VLAN IDs greater than 1005) to the allowed 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 4094; extended-range VLAN IDs are valid.  
Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.
- **except** lists the VLANs that should be calculated by inverting the defined list of VLANs. (VLANs are added except the ones specified.) Valid IDs are from 1 to 1005. Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.
- *vlan-atom* is either a single VLAN number from 1 to 4094 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen.

## Defaults

VLAN 1 is the default native VLAN ID on the port.

The default for all VLAN lists is to include all VLANs.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

**Usage Guidelines**

Native VLANs:

- All untagged traffic received on an IEEE 802.1Q trunk port is forwarded with the native VLAN configured for the port.
- If a packet has a VLAN ID that is the same as the sending-port native VLAN ID, the packet is sent without a tag; otherwise, the switch sends the packet with a tag.
- The **no** form of the **native vlan** command resets the native mode VLAN to the appropriate default VLAN for the device.

Allowed VLAN:

- To reduce the risk of spanning-tree loops or storms, you can disable VLAN 1 on any individual VLAN trunk port by removing VLAN 1 from the allowed list. When you remove VLAN 1 from a trunk port, the interface continues to send and receive management traffic, for example, Cisco Discovery Protocol (CDP), Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), Dynamic Trunking Protocol (DTP), and VLAN Trunking Protocol (VTP) in VLAN 1.
- The **no** form of the **allowed vlan** command resets the list to the default list, which allows all VLANs.

**Examples**

This example shows how to configure VLAN 3 as the default for the port to send all untagged traffic:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport trunk native vlan 3
```

This example shows how to add VLANs 1, 2, 5, and 6 to the allowed list:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport trunk allowed vlan add 1,2,5,6
```

You can verify your settings by entering the **show interfaces *interface-id* switchport** privileged EXEC command.

**Related Commands**

Command	Description
<a href="#">show interfaces switchport</a>	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
<a href="#">switchport mode</a>	Configures the VLAN membership mode of a port.

## switchport vlan mapping

To configure VLAN mapping on a trunk port, use the **switchport vlan mapping** interface configuration command with the **dot1q tunnel** keywords. You can configure one-to-one VLAN mapping, 802.1Q tunneling (QinQ) mapping, or selective QinQ mapping. To configure all-to-one or selective VLAN mapping on an 802.1ad C-UNI trunk port, use the command with the **dot1ad-bundle** keyword. Use the **no** form of the command to disable the configuration.

```
switchport vlan mapping vlan-id {translated-id | dot1ad-bundle outer vlan id | dot1q tunnel translated-id}
```

```
no switchport vlan mapping vlan-id {translated-id | dot1ad-bundle outer vlan id | dot1q tunnel translated-id}
```

```
switchport vlan mapping default {dot1ad-bundle outer vlan id | dot1q tunnel translated-id | drop}}
```

```
no switchport vlan mapping default {dot1ad-bundle outer vlan id | dot1q tunnel translated-id | drop}}
```

```
no switchport vlan mapping all
```

### Syntax Description

<i>vlan-id</i>	Specify the original (customer) VLAN or VLANs (C-VLANs), also known as the VLAN on the wire, for one-to-one or selective QinQ mapping. You can enter multiple VLAN IDs separated by a comma or a series of VLAN IDs separated by a hyphen (for example 1,2,3-5). The range is from 1 to 4094.
<i>translated-id</i>	Specify the translated VLAN-ID: the S-VLAN to be used in the service provider network. The range is from 1 to 4094.
<b>default</b>	Specify the default for C-VLANs other than those specified.
<b>dot1ad-bundle</b> <i>outer vlan-id</i>	Specifies 802.1ad bundling on an 802.1ad C-UNI trunk port. <ul style="list-style-type: none"> <li>Enter after the <b>default</b> keyword to select all-to-one bundling.</li> <li>Enter after <i>vlan-id</i> to select selective bundling.</li> </ul> <p>The outer VLAN ID range is from 1 to 4094.</p> <p><b>Note</b> This command is available only on 802.1ad trunk C-UNI ports.</p>
<b>dot1q-tunnel</b> <i>translated-id</i>	Add a translated VLAN-ID to specify a VLAN tunnel (add an outer S-VLAN tag). The range of the S-VLAN tag is 1 to 4094. Use these keywords for traditional QinQ mapping.
<b>drop</b>	Specify that VLANs other than the C-VLAN or VLANs specified are dropped. Use this keyword for one-to-one or selective QinQ mapping.
<b>all</b>	In the <b>no switchport vlan mapping</b> command, specifies that all VLAN mapping configurations on the interface are deleted.

### Defaults

No VLAN mapping is configured.



**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.
	12.2(54)SE	The <b>dot1ad-bundle</b> <i>outer vlan id</i> keywords were added.

### Usage Guidelines

Before configuring VLAN mapping on an interface, enter the **switchport mode trunk** interface configuration command to configure the interface as a trunk port.

You configure VLAN mapping on ports connected to the customer network, which are typically user network interfaces (UNIs). However, you can also configure VLAN mapping on a network node interface (NNI) or on an enhanced network interface (ENI).

For 802.1ad, VLAN mapping is permitted only on 802.1ad C-UNI trunk ports. VLAN mapping is not supported on S-UNI and NNI interfaces.

You can configure VLAN mapping on a physical interface or on a port channel of multiple interfaces with the same configuration.

For 802.1Q VLAN mapping:

- To configure one-to-one VLAN mapping, use the **switchport vlan mapping** *vlan-id translated-id* command.
- To configure traditional QinQ (VLAN bundling) on an interface, enter the **switchport vlan mapping default dot1q-tunnel** *outer vlan-id*. This is the same as configuring the interface as a tunnel port and maps all VLANs to the specified S-VLAN ID.



**Note** To avoid mixing customer traffic, when you configure traditional QinQ on a trunk port, you should use the **switchport trunk allowed vlan** *vlan-id* interface configuration command to configure the outer VLAN ID (S-VLAN) as an allowed VLAN on the trunk port.

- To configure selective QinQ on an interface, enter the **switchport vlan mapping** *vlan-id dot1q-tunnel* *outer vlan-id* command.

You can configure one-to-one mapping and selective QinQ on the same interface, but you cannot use the same C-VLAN IDs in both configurations.

For one-to-one mapping and selective QinQ, or for default all-to-one 802.1ad VLAN mapping, you can use the **default drop** keywords to specify that traffic is dropped unless the specified C-VLAN ID and S-VLAN ID combination is explicitly translated.

The **no** form of the **switchport vlan mapping** commands clears the specified mapping configuration on the interface. The **no switchport vlan mapping all** command clears all mapping configurations on the interface.

On an ME-3400E interface configured for VLAN mapping, mapping to the S-VLAN occurs on traffic entering the switch. Therefore, when you configure other features on an interface configured for VLAN mapping and a VLAN ID is required, use the S-VLAN ID. The exception is when configuring VLAN mapping and Ethernet E-LMI on an interface. Use the C-VLAN in the **ethernet lmi ce-vlan map** *vlan-id* service-instance configuration mode command.

You cannot configure **encapsulation replicate** on a SPAN destination port if the source port is configured as a tunnel port or has a one-to-two mapping configured. Encapsulation replicate is supported with one-to-one VLAN mapping.

For VLAN mapping on 802.1ad C-UNI trunk ports:

- You use the **dot1ad-bundle** keywords to achieve all-to-one and selective bundling functionality on a C-UNI trunk port. The default mapping is one-to-one on the source VLAN.
- You can configure 802.1ad only on C-UNI trunk ports. This command is not supported on S-UNIs or NNIs.

## Examples

This example shows how to use one-to-one mapping to map VLAN IDs 1 and 2 in the customer network to VLANs 1001 and 1002 in the service-provider network and to drop traffic from any other VLAN IDs.

```
Switch(config)# interface gigabitEthernet0/1
Switch(config-if)# switchport vlan mapping 1 1001
Switch(config-if)# switchport vlan mapping 2 1002
Switch(config-if)# switchport vlan mapping default drop
Switch(config-if)# exit
```

This example shows how to use traditional QinQ to bundle all traffic on the port to leave the switch with an S-VLAN ID of 10.

```
Switch(config)# interface gigabitEthernet0/1
Switch(config-if)# switchport vlan mapping default dot1q-tunnel 10
Switch(config-if)# exit
```

This example shows how to configure selective QinQ mapping on the port so that traffic with a C-VLAN ID of 5, 7, or 8 would enter the switch with an S-VLAN ID of 100. The traffic of any other VLAN IDs is dropped.

```
Switch(config)# interface gigabitEthernet0/1
Switch(config-if)# switchport vlan mapping 5, 7-8 dot1q-tunnel 100
Switch(config-if)# switchport vlan mapping default drop
Switch(config-if)# exit
```

This example shows how to configure default all-to-one 802.1ad VLAN mapping on a C-UNI port:

```
Switch (config)# interface GigabitEthernet0/2
Switch (config-if)# switchport access vlan 4002
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan 4002
Switch (config-if)# switchport vlan mapping default dot1ad-bundle 4002
Switch (config-if)# Ethernet dot1ad uni c-port
Switch(config-if)# exit
```

This example shows how to configure selective 802.1ad VLAN mapping on the port.

```
Switch(config)# interface gigabitEthernet0/1
Switch (config-if)# switchport mode trunk
Switch(config-if)# switchport vlan mapping 5, 7-8 dot1ad-bundle 100
Switch(config-if)# switchport vlan mapping default drop
Switch (config-if)# Ethernet dot1ad uni c-port
Switch(config-if)# exit
```

## Related Commands

Command	Description
<a href="#">show vlan mapping</a>	Displays VLAN mapping information.

# system env temperature threshold yellow

Use the **system env temperature threshold yellow** global configuration command to configure the difference between the yellow and red temperature thresholds which determines the value of yellow threshold. Use the no form of this command to return to the default value.

**system env temperature threshold yellow** *value*

**no system env temperature threshold yellow** *value*

## Syntax Description

*value* Specify the difference between the yellow and red threshold values (in Celsius). The range is 8 to 25. The default value is 10.

## Defaults

The default value is 10.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

You cannot configure the green and red thresholds but can configure the yellow threshold. Use the **system env temperature threshold yellow** *value* global configuration command to specify the difference between the yellow and red thresholds and to configure the yellow threshold. For example, if the red threshold is 66 degrees C and you want to configure the yellow threshold as 51 degrees C, set the difference between the thresholds as 15 by using the **system env temperature threshold yellow 15** command.



### Note

The internal temperature sensor in the switch measures the internal system temperature and might vary  $\pm 5$  degrees C.

## Examples

This example sets 15 as the difference between the yellow and red thresholds:

```
Switch(config)# system env temperature threshold yellow 15
Switch(config)#
```

## Related Commands

Command	Description
<b>show env temperature</b>	Displays the switch temperature status and thresholds.

## system mtu

Use the **system mtu** global configuration command to set the maximum packet size or maximum transmission unit (MTU) size for Gigabit Ethernet ports or for Fast Ethernet (10/100) ports or to set an alternate MTU for specific ports. Use the **no** form of this command to restore the global MTU value to its default value.

**system mtu** { *bytes* | **alternate** { *bytes* | **interface** *interface-id* } | **jumbo** *bytes* | **routing** *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. The default is 1500 bytes. This is the maximum MTU received at 10/100-Mb/s Ethernet switch ports.
<b>alternate</b> <i>bytes</i>		Define an alternate frame size (MTU) to be applied to specific interfaces. The range is between the configured system MTU and the configured jumbo MTU size (1500 to 9000 bytes). The default is 1500 bytes.
<b>alternate interface</b> { <i>interface-id</i>   <b>range</b> <i>interface-range</i> }		Apply the alternate MTU to the specified interface or range of interfaces.
<b>jumbo</b> <i>bytes</i>		Set the system jumbo frame size (MTU) for Gigabit Ethernet ports. The range is 1500 to 9000 bytes. The default is 1500 bytes. This is the maximum MTU received at the physical port for Gigabit Ethernet ports.
<b>routing</b> <i>bytes</i>		Set the maximum MTU for routed packets. You can also set the maximum MTU to be advertised by the routing protocols that support the configured MTU size. The range is 1500 bytes to the system MTU value. The system routing MTU is the maximum MTU for routed packets and is also the maximum MTU that the switch advertises in routing updates for protocols such as OSPF.

### Defaults

The default MTU size for all ports is 1500 bytes. However, if you configure a different value for the system MTU, that configured value becomes the default MTU size for routed ports when it is applied following a switch reset.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(44)EY	This command was introduced.
12.2(55)SE	The <b>alternate</b> { <i>bytes</i>   <b>interface</b> <i>interface-id</i> } keywords <i>were</i> introduced.

**Usage Guidelines**

When you use this command to change the system MTU or jumbo MTU, or to set an alternate MTU size, you must reset the switch before the new configuration takes effect. The **system mtu routing** command does not require a switch reset to take effect.

**Note**

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** 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 do not configure the **system mtu jumbo** command, the setting of the **system mtu** command applies to all Gigabit Ethernet interfaces.

You can use the **system mtu routing** command to configure the MTU size on routed ports.

**Note**

You cannot configure a routing MTU size that exceeds the system MTU size. If you change the system MTU size to a value smaller than the currently configured routing MTU size, the configuration change is accepted, but not applied until the next switch reset. When the configuration change takes effect, the routing MTU size defaults to the new system MTU size.

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

Beginning with Cisco IOS Release 12.2(55)SE, you can define an alternate MTU size by using the **system mtu alternate bytes** command and apply it to specified interfaces by using the **system mtu alternate interface interface-id** command. You can define only one alternate MTU size per switch, but you can apply it to multiple interfaces. The alternate MTU cannot be greater than the jumbo MTU size set on the switch. When you apply an alternate MTU size to an interface, frames received on the interface that are greater than the alternate MTU size are dropped.

You can apply the alternate MTU size to Fast Ethernet or Gigabit Ethernet interfaces, but if the alternate MTU size is greater than 1998 bytes, you cannot apply it to Fast Ethernet interfaces. The alternate MTU size has no effect on the routing MTU size.

The size of frames that can be received by the switch CPU is limited to 1998 bytes, regardless of the value entered with the **system mtu** command. Although forwarded or routed frames are usually not received by the CPU, some packets (for example, control traffic, SNMP, Telnet, and routing protocols) are sent to the CPU.

Because the switch does not fragment packets, it drops:

- switched packets larger than the packet size supported on the *egress* interface
- routed packets larger than the routing MTU value

For example, if the **system mtu** value is 1998 bytes and the **system mtu jumbo** value is 5000 bytes, packets up to 5000 bytes can be received on interfaces operating at 1000 Mb/s. However, although a packet larger than 1998 bytes can be received on an interface operating at 1000 Mb/s, if its destination interface is operating at 10 or 100 Mb/s, the packet is dropped.

**Examples**

This example shows how to set the maximum packet size for Gigabit Ethernet ports to 1800 bytes:

```
Switch(config)# system mtu jumbo 1800
Switch(config)# exit
Switch# reload
```

This example shows how to set the maximum packet size for Gigabit Ethernet ports to 1800 bytes, to define an alternate MTU size of 1700 bytes and apply it to Gigabit Ethernet port 0/8. Changes are not applied until you reload the switch:

```
Switch(config)# system mtu jumbo 1800
Switch(config)# system mtu alternate 1700
Changes to the Alternate MTU will not take effect until the next reload is done
Switch(config)# system mtu alternate interface gigabitethernet 0/8
Changes to the Alternate MTU on interface will not take effect until the next re
load is done
Switch(config)# exit
Switch# reload
```

This example shows how to apply the alternate MTU to Gigabit Ethernet interfaces 1 to 10. Changes are not applied until you reload the switch:

```
Switch(config)# system mtu alternate interface range gigabitethernet 0/1-10
Changes to the Alternate MTU on interface(s) will not take effect until the next reload is done
Switch(config)# exit
```

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

**Related Commands**

Command	Description
<b>show interface <i>interface-id</i> mtu</b>	Displays the MTU setting on the specified interface.
<b>show system mtu</b>	Displays the packet size set for Fast Ethernet and Gigabit Ethernet ports.

# table-map

Use the **table-map** global configuration command to create a quality of service (QoS) mapping and to enter table-map configuration mode. Table maps can be specified in policy-map class **set** commands or as mark down mappings for policers and are used to create and configure a mapping table for converting one packet-marking value to another. Use the **no** form of this command to delete the mapping table.

**table-map** *table-map-name*

**no table-map** *table-map-name*

Syntax Description	
	<i>class-map-name</i> Name of the table map.

Defaults	
	No table maps are defined.

Command Modes	
	Global configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

Usage Guidelines	
	Use this command to specify the name of the table map that you want to create or to modify and to enter table-map configuration mode.

You use the **table-map** command to create a mapping table, which is a type of conversion chart used for establishing a *to-from* relationship between packet-marking types or categories. For example, you can use a mapping table to establish a to-from relationship among these categories:

- class of service (CoS)
- precedence
- Differentiated Services Code Point (DSCP)

The switch supports a maximum of 256 unique table maps.

The maximum number of map statements within a table map is 64.

After you are in table-map configuration mode, these configuration commands are available:

- **default**: the default behavior for setting a value not found in the table map. The default can be specified as one of these:
  - *default value*—uses the table map default value. The range is from 0 to 63.
  - **copy**—sets the default behavior for a value not found in the table map to copy.
  - **ignore**—sets the default behavior for a value not found in the table map to ignore.
- **exit**: exits from QoS table-map configuration mode.
- **map**: the table map **from** *from\_value* and **to** *to\_value*. Both value ranges are from 0 to 63.
- **no**: deletes the table map or sets the default values.

You can specify table maps in **set** commands and use them as mark-down mapping for the policers in input policy maps.

You cannot use table maps in output policy maps.

### Examples

This example shows how to create a table map to map DSCP to CoS values, setting those DSCP values that are not mapped to a CoS value of 4:

```
Switch(config)# table-map dscp-to-cos
Switch(config-tablemap)# map from 1 to 1
Switch(config-tablemap)# map from 2 to 1
Switch(config-tablemap)# map from 3 to 1
Switch(config-tablemap)# map from 4 to 2
Switch(config-tablemap)# map from 5 to 2
Switch(config-tablemap)# map from 6 to 3
Switch(config-tablemap)# default 4
Switch(config-tablemap)# exit
```

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

### Related Commands

Command	Description
<a href="#">class</a>	Defines a traffic classification match criteria for the specified class-map name.
<a href="#">policy-map</a>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
<a href="#">set cos</a>	Classifies IP traffic by setting a CoS, DSCP, IP-precedence, or QoS group value in the packet.
<a href="#">Related Commands</a>	Displays QoS table maps.



# test cable-diagnostics tdr

Use the **test cable-diagnostics tdr** privileged EXEC command to run the Time Domain Reflector (TDR) feature on an interface.

**test cable-diagnostics tdr interface** *interface-id*



## Note

TDR is supported only on the copper Ethernet 10/100 or 10/100/100 ports on the Cisco ME switch. This includes dual-purpose ports that are configured as 10/100/1000 ports by using the RJ-45 connector.

## Syntax Description

<i>interface-id</i>	Specify the interface on which to run TDR.
---------------------	--

## Defaults

There is no default.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

You can use the TDR feature to diagnose and resolve cabling problems. TDR is supported only on copper Ethernet 10/100 or 10/100/1000 ports. It is not supported on small form-factor pluggable (SFP) module ports. For more information about TDR, see the software configuration guide for this release.

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.

## Examples

This example shows how to run TDR on an interface:

```
Switch# test cable-diagnostics tdr interface gigabitethernet0/2
TDR test started on interface Gi0/2
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 status of up and a speed of 10 or 100 Mbps, these messages appear:

```
Switch# test cable-diagnostics tdr interface gigabitethernet0/3
TDR test on Gi0/9 will affect link state and traffic
TDR test started on interface Gi0/3
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

**■** test cable-diagnostics tdr

Related Commands	Command	Description
	<a href="#">show cable-diagnostics tdr</a>	Displays the TDR results.

# traceroute mac

Use the **traceroute mac** privileged EXEC command to display the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address.

```
traceroute mac [interface interface-id] {source-mac-address} [interface interface-id]
  {destination-mac-address} [vlan vlan-id] [detail]
```



## Note

Layer 2 traceroute is available only on network node interfaces (NNIs).

## Syntax Description

<b>interface</b> <i>interface-id</i>	(Optional) Specify an interface on the source or destination switch.
<b>source-mac-address</b>	Specify the MAC address of the source switch in hexadecimal format.
<i>destination-mac-address</i>	Specify the MAC address of the destination switch in hexadecimal format.
<b>vlan</b> <i>vlan-id</i>	(Optional) Specify the VLAN on which to trace the Layer 2 path that the packets take from the source switch to the destination switch. Valid VLAN IDs are 1 to 4094.
<b>detail</b>	(Optional) Specify that detailed information appears.

## Defaults

There is no default.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on all the switches in the network. Do not disable CDP.



## Note

Layer 2 traceroute is available only on NNIs.

When the switch detects a device in the Layer 2 path that does not support Layer 2 traceroute, the switch continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

Layer 2 traceroute supports only unicast traffic. If you specify a multicast source or destination MAC address, the physical path is not identified, and an error message appears.

The **traceroute mac** command output shows the Layer 2 path when the specified source and destination addresses belong to the same VLAN. If you specify source and destination addresses that belong to different VLANs, the Layer 2 path is not identified, and an error message appears.

If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong. If the VLAN is not specified, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port). When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

## Examples

This example shows how to display the Layer 2 path by specifying the source and destination MAC addresses:

```
Switch# tracert mac 0000.0201.0601 0000.0201.0201
Source 0000.0201.0601 found on con6[ME-3400-24TS] (2.2.6.6)
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5          (2.2.5.5      ) :   Gi0/3 => Gi0/1
con1          (2.2.1.1      ) :   Gi0/1 => Gi0/2
con2          (2.2.2.2      ) :   Gi0/2 => Gi0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

This example shows how to display the Layer 2 path by using the **detail** keyword:

```
Switch# tracert mac 0000.0201.0601 0000.0201.0201 detail
Source 0000.0201.0601 found on con6[ME-3400-24TS] (2.2.6.6)
ME-3400-24TS / 2.2.6.6 :
    Gi0/2 [auto, auto] => Gi0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
    Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
    Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
    Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the interfaces on the source and destination switches:

```
Switch# tracert mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3 0000.0201.0201
Source 0000.0201.0601 found on con6[ME-3400-24TS] (2.2.6.6)
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5          (2.2.5.5      ) :   Gi0/3 => Gi0/1
con1          (2.2.1.1      ) :   Gi0/1 => Gi0/2
con2          (2.2.2.2      ) :   Gi0/2 => Gi0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

This example shows the Layer 2 path when the switch is not connected to the source switch:

```
Switch# traceroute mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source .....
Source 0000.0201.0501 found on con5[ME-3400-24TS] (2.2.5.5)
con5 / ME-3400-24TS/ 2.2.5.5 :
    Gi0/1 [auto, auto] => Gi0/3 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
    Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
    Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows the Layer 2 path when the switch cannot find the destination port for the source MAC address:

```
Switch# traceroute mac 0000.0011.1111 0000.0201.0201
Error:Source Mac address not found.
Layer2 trace aborted.
```

This example shows the Layer 2 path when the source and destination devices are in different VLANs:

```
Switch# traceroute mac 0000.0201.0601 0000.0301.0201
Error:Source and destination macs are on different vlans.
Layer2 trace aborted.
```

This example shows the Layer 2 path when the destination MAC address is a multicast address:

```
Switch# traceroute mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
```

This example shows the Layer 2 path when source and destination switches belong to multiple VLANs:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace aborted.
```

## Related Commands

Command	Description
<a href="#">traceroute mac ip</a>	Displays the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname.

# tracert mac ip

Use the **tracert mac ip** privileged EXEC command to display the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname.

```
tracert mac ip {source-ip-address | source-hostname} {destination-ip-address | destination-hostname} [detail]
```



## Note

Layer 2 tracert is available only on network node interfaces (NNIs).

## Syntax Description

<b>source-ip-address</b>	Specify the IP address of the source switch as a 32-bit quantity in dotted-decimal format.
<i>destination-ip-address</i>	Specify the IP address of the destination switch as a 32-bit quantity in dotted-decimal format.
<i>source-hostname</i>	Specify the IP hostname of the source switch.
<i>destination-hostname</i>	Specify the IP hostname of the destination switch.
<b>detail</b>	(Optional) Specify that detailed information appears.

## Defaults

There is no default.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

For Layer 2 tracert to function properly, Cisco Discovery Protocol (CDP) must be enabled on all the switches in the network. Do not disable CDP.



## Note

Layer 2 tracert is available only on network node interfaces (NNIs).

When the switch detects an device in the Layer 2 path that does not support Layer 2 tracert, the switch continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

The **tracert mac ip** command output shows the Layer 2 path when the specified source and destination IP addresses are in the same subnet. When you specify the IP addresses, the switch uses Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.

- If an ARP entry exists for the specified IP address, the switch uses the associated MAC address and identifies the physical path.

- If an ARP entry does not exist, the switch sends an ARP query and tries to resolve the IP address. The IP addresses must be in the same subnet. If the IP address is not resolved, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port). When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

## Examples

This example shows how to display the Layer 2 path by specifying the source and destination IP addresses and by using the **detail** keyword:

```
Switch# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / ME-3400-24TS- / 2.2.6.6 :
    Gi0/1 [auto, auto] => Gi0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
    Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
    Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
    Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the source and destination hostnames:

```
Switch# traceroute mac ip con6 con2
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5          (2.2.5.5      ) :   Gi0/3 => Gi0/1
con1          (2.2.1.1      ) :   Gi0/1 => Gi0/2
con2          (2.2.2.2      ) :   Gi0/2 => Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
```

This example shows the Layer 2 path when ARP cannot associate the source IP address with the corresponding MAC address:

```
Switch# traceroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
```

## Related Commands

Command	Description
<a href="#">shutdown</a>	Displays the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address.

# udld

Use the **udld** global configuration command to enable aggressive or normal mode in the UniDirectional Link Detection (UDLD) and to set the configurable message timer time. Use the **no** form of the command to disable aggressive or normal mode UDLD on all fiber-optic ports.

**udld** { **aggressive** | **enable** | **message time** *message-timer-interval* }

**no udld** { **aggressive** | **enable** | **message** }

## Syntax Description

<b>aggressive</b>	Enable UDLD in aggressive mode on all fiber-optic interfaces.
<b>enable</b>	Enable UDLD in normal mode on all fiber-optic interfaces.
<b>message time</b> <i>message-timer-interval</i>	Configure the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is 7 to 90 seconds.

## Defaults

UDLD is disabled on all interfaces.  
The message timer is set at 15 seconds.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links. For information about normal and aggressive modes, see the “Understanding UDLD” section in the software configuration guide for this release.

If you change the message time between probe packets, you are making a trade-off between the detection speed and the CPU load. By decreasing the time, you can make the detection-response faster but increase the load on the CPU.

This command affects fiber-optic interfaces only. Use the **udld** interface configuration command to enable UDLD on other interface types.

You can use these commands to reset an interface shut down by UDLD:

- The **udld reset** privileged EXEC command to reset all interfaces shut down by UDLD
- The **shutdown** and **no shutdown** interface configuration commands
- The **no udld enable** global configuration command followed by the **udld** { **aggressive** | **enable** } global configuration command to re-enable UDLD globally



- The **no udld port** interface configuration command followed by the **udld port** or **udld port aggressive** interface configuration command to re-enable UDLD on the specified interface
- The **errdisable recovery cause udld** and **errdisable recovery interval *interval*** global configuration commands to automatically recover from the UDLD error-disabled state

---

### Examples

This example shows how to enable UDLD on all fiber-optic interfaces:

```
Switch(config)# udld enable
```

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

---

### Related Commands

Command	Description
<a href="#">show udld</a>	Displays UDLD administrative and operational status for all ports or the specified port.
<a href="#">udld port</a>	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the <b>udld</b> global configuration command.
<a href="#">udld reset</a>	Resets all interfaces shut down by UDLD and permits traffic to again pass through.

# udld port

Use the **udld port** interface configuration command to enable the UniDirectional Link Detection (UDLD) on an individual interface or prevent a fiber-optic interface from being enabled by the **udld** global configuration command. Use the **no** form of this command to return to the **udld** global configuration command setting or to disable UDLD if entered for a nonfiber-optic port.

**udld port [aggressive]**

**no udld port [aggressive]**

## Syntax Description

<b>aggressive</b>	Enable UDLD in aggressive mode on the specified interface.
-------------------	--

## Defaults

On fiber-optic interfaces, UDLD is not enabled, not in aggressive mode, and not disabled. For this reason, fiber-optic interfaces enable UDLD according to the state of the **udld enable** or **udld aggressive** global configuration command.

On nonfiber-optic interfaces, UDLD is disabled.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another switch. If the port is a user network interface (UNI) or enhanced network interface (ENI), you must use the **no shutdown** interface configuration command to enable it before using the **udld port** command. UNIs and ENIs are disabled by default. Network node interfaces (NNIs) are enabled by default.

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links. For information about normal and aggressive modes, see the “Configuring UDLD” chapter in the software configuration guide for this release.

To enable UDLD in normal mode, use the **udld port** interface configuration command. To enable UDLD in aggressive mode, use the **udld port aggressive** interface configuration command.

Use the **no udld port** command on fiber-optic ports to return control of UDLD to the **udld enable** global configuration command or to disable UDLD on nonfiber-optic ports.

Use the **udld port aggressive** command on fiber-optic ports to override the setting of the **udld enable** or **udld aggressive** global configuration command. Use the **no** form on fiber-optic ports to remove this setting and to return control of UDLD enabling to the **udld** global configuration command or to disable UDLD on nonfiber-optic ports.

If the switch software detects a small form-factor pluggable (SFP) module change and the port changes from fiber optic to nonfiber optic or the reverse, all configurations are maintained.

You can use these commands to reset an interface shut down by UDLD:

- The **udld reset** privileged EXEC command to reset all interfaces shut down by UDLD
- The **shutdown** and **no shutdown** interface configuration commands
- The **no udld enable** global configuration command followed by the **udld {aggressive | enable}** global configuration command to re-enable UDLD globally
- The **no udld port** interface configuration command followed by the **udld port** or **udld port aggressive** interface configuration command to re-enable UDLD on the specified interface
- The **errdisable recovery cause udld** and **errdisable recovery interval *interval*** global configuration commands to automatically recover from the UDLD error-disabled state

### Examples

This example shows how to enable UDLD on an port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# udld port
```

This example shows how to disable UDLD on a fiber-optic interface despite the setting of the **udld** global configuration command:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no udld port
```

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

### Related Commands

Command	Description
<b>show running-config</b>	Displays the operating configuration.
<b>show udld</b>	Displays UDLD administrative and operational status for all ports or the specified port.
<b>udld</b>	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
<b>udld reset</b>	Resets all interfaces shut down by UDLD and permits traffic to again pass through.

# udld reset

Use the **udld reset** privileged EXEC command to reset all interfaces disabled by the UniDirectional Link Detection (UDLD) and permit traffic to begin passing through them again (though other features, such as spanning tree and Port Aggregation Protocol (PAgP) still have their normal effects, if enabled).

## udld reset



### Note

PAgP is available only on network node interfaces (NNIs) and enhanced network interfaces (ENIs).

### Syntax Description

This command has no arguments or keywords.

### Command Modes

Privileged EXEC

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

If the interface configuration is still enabled for UDLD, these ports begin to run UDLD again and are disabled for the same reason if the problem has not been corrected.

### Examples

This example shows how to reset all interfaces disabled by UDLD:

```
Switch# udld reset
1 ports shutdown by UDLD were reset.
```

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

### Related Commands

Command	Description
<b>show running-config</b>	Displays the operating configuration.
<b>show udld</b>	Displays UDLD administrative and operational status for all ports or the specified port.
<b>udld</b>	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
<b>udld port</b>	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the <b>udld</b> global configuration command.

# uni count

Use the **uni count** EVC configuration command to set the user-network interface (UNI) count for an Ethernet virtual connection (EVC). Use the **no** form of this command to return to the default setting.

**uni count** *value* [**multipoint**]

**no uni count**

## Syntax Description

<i>value</i>	Set the number of UNIs in the EVC. The range is from 1 to 1024. The default is 2.
<b>multipoint</b>	(Optional) Select point-to-multipoint service. This keyword is visible only when you enter a <b>uni count</b> value of 2. <ul style="list-style-type: none"> <li>If you do not enter a value or if you enter 1 or 2, the service defaults to point-to-point service. If you enter 2, you can configure point-to-multipoint service.</li> <li>If you enter a <b>uni count</b> value of 3 or greater, the service is point-to-multipoint.</li> </ul>

## Defaults

The default UNI count is 2. The default service, if you do not enter a UNI count, is point-to-multipoint.

## Command Modes

EVC configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The UNI count determines the type of service in the EVC.

- If the command is not entered, the UNI count defaults to 2 and the service defaults to point-to-point service.
- If you manually enter a value of 2, you can leave the service at the default or can configure point-to-multipoint service by entering the **multipoint** keyword.
- If you enter a value of 3 or greater, the service is point-to-multipoint.

You should know the correct number of maintenance end points (MEPs) in the domain. If you enter a UNI count value greater than the actual number of endpoints, the UNI status shows as partially active even if all endpoints are up. If you enter a UNI count less than the actual number of endpoints, UNI status shows as active, even if all endpoints are not up.



### Caution

Configuring a UNI count does not prevent you from configuring more endpoints than the configured count. For example, if you configure a UNI count of five, but you create ten MEPs, any five MEPs in the domain can go down without the status changing to Partially Active.

---

**Examples**

This example shows how to a UNI count of two with point-to-multipoint service:

```
Switch(config)# ethernet evc test1
Switch(config-enc)# uni count 2 multipoint
```

---

**Related Commands**

Command	Description
<a href="#">ethernet evc</a> <i>evc-id</i>	Defines an EVC and enters EVC configuration mode.

---

# uni-vlan

Use the **uni-vlan** VLAN configuration command to configure the VLAN as a user network interface-enhanced network interface (UNI-ENI) community or isolated VLAN. UNIs and ENIs on a switch that are assigned to a community VLAN can exchange packets with one another; UNIs and ENIs in an isolated VLAN cannot exchange packets. Use the **no** form of this command to return the VLAN to the default UNI-ENI isolated VLAN.

**uni-vlan {community | isolated}**

**no uni-vlan**

Syntax Description	community	Designate the UNI-ENI VLAN as a community VLAN.
	<b>isolated</b>	Designate the UNI-ENI VLAN as an isolated VLAN.

**Defaults** The default VLAN configuration is UNI-ENI isolated VLAN.

**Command Modes** VLAN configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** In a UNI-ENI isolated VLAN, packets are not exchanged between UNIs or ENIs within the VLAN. Packets can be exchanged between UNIs or ENIs and network node interfaces (NNIs) in the same UNI isolated VLAN.

In a UNI-ENI community VLAN, packets can be exchanged between UNIs, between ENIs, or between UNIs and NNIs in the same community VLAN. However, there can be no more than a combined total of eight UNIs and ENIs in a UNI community VLAN.



**Note** Local switching takes place between ENIs and UNIs in the same community VLAN. Because you can enable spanning tree on ENIs, but not on UNIs, you should use caution when configuring ENIs and UNIs in the same community VLAN. UNIs are always in the forwarding state.

VLAN 1 is always a UNI-ENI isolated VLAN; you cannot configure VLAN 1 as a UNI-ENI community VLAN. The reserved VLANs, 1002 to 1005, are not Ethernet VLANs.

As with any other VLAN, you can statically assign ports to UNI-ENI VLANs by using the **switchport access vlan vlan-id** interface configuration command. Ports are also dynamically assigned to UNI-ENI VLANs.

The **uni-vlan** command does not take effect until you exit from VLAN configuration mode.

A UNI-ENI VLAN cannot be a Remote Switched Port Analyzer (RSPAN) VLAN.

A UNI-ENI VLAN cannot be a private VLAN.

To change a UNI-ENI isolated VLAN to an RSPAN VLAN or a private VLAN, enter the **rspan-vlan** or **private-vlan** VLAN configuration command. This overwrites the default isolated VLAN configuration. To change a UNI-ENI community VLAN to an RSPAN VLAN or a private VLAN, you must first enter the **no uni-vlan** VLAN configuration command to return to the default UNI-ENI isolated VLAN configuration before entering the **rspan-vlan** or **private-vlan** VLAN configuration command.

**Note**

For more information about UNI-ENI VLANs and interaction with other features, see the software configuration guide for this release.

**Examples**

This example shows how to change VLAN 20 from the default UNI-ENI isolated VLAN to a UNI-ENI community VLAN:

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# uni-vlan community
Switch(config-vlan)# exit
```

You can verify your setting by entering the **show vlan uni-vlan** or **show vlan *vlan-id* uni-vlan [type]** privileged EXEC command.

**Related Commands**

Command	Description
<b>show interfaces status</b>	Displays the status of interfaces, including the VLANs to which they belong.
<b>show vlan uni-vlan</b>	Displays the UNI-ENI VLANs on the switch.



# violate-action

Use the **violate-action** policy-map class police configuration command to set multiple actions for a policy-map class for packets with a rate greater than the conform rate plus the exceed burst for the committed information rate (CIR) or peak information rate (PIR). Use the **no** form of this command to cancel the action or to return to the default action.

```
violate-action { drop | set-cos-transmit { new-cos-value | [cos | dscp | precedence] [table table-map name]} | set-dscp-transmit { new-dscp-value | [cos | dscp | precedence] [table table-map name]} | set-prec-transmit { new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-qos-transmit qos-group-value | transmit }
```

```
no violate-action { drop | set-cos-transmit { new-cos-value | [cos | dscp | precedence] [table table-map name]} | set-dscp-transmit { new-dscp-value | [cos | dscp | precedence] [table table-map name]} | set-prec-transmit { new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-qos-transmit qos-group-value | transmit }
```

Syntax	Description
<b>drop</b>	Drop the packet.
<b>set-cos-transmit</b> <i>new-cos-value</i>	Set a new class of service (CoS) value for the packet, and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new CoS value is 0 to 7.
<b>set-dscp-transmit</b> <i>new-dscp-value</i>	Set a new Differentiated Services Code Point (DSCP) value for the packet, and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new DCSP value is 0 to 63.
<b>set-prec-transmit</b> <i>new-precedence-value</i>	Set a new IP precedence value for the packet, and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new IP precedence value is 0 to 7.
<b>set-qos-transmit</b> <i>qos-group-value</i>	Set a new quality of service (QoS) group value for the packet, and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new QoS value is 0 to 99.
<b>cos</b>	(Optional) Set the packet marking specified in the preceding keyword based on the CoS value of the incoming packet, and send the packet. This specifies the <i>from-type</i> of the enhanced packet-marking action.
<b>dscp</b>	(Optional) Set the packet marking specified in the preceding keyword based on the DSCP value of the incoming packet, and send the packet. This specifies the <i>from-type</i> of the enhanced packet-marking action.
<b>precedence</b>	(Optional) Set the packet marking specified in the preceding keyword based on the IP precedence value of the incoming packet, and send the packet. This specifies the <i>from-type</i> of the enhanced packet-marking action.
<b>table</b> <i>table-map name</i>	(Optional) Used with the preceding <i>from-type</i> keyword. Specify the table map to be used for the enhanced packet marking. The <i>to-type</i> of the action is marked based on the <i>from-type</i> parameter of the action using this table map.
<b>transmit</b>	(Optional) Send the packet unmodified.

## Defaults

The default action is to drop the packet.

## violate-action

**Command Modes** Policy-map class police configuration

**Command History**

Release	Modification
12.2(44)EY	This command was introduced.

**Usage Guidelines**

You configure violate actions for packets when the packet rate is greater than the conform rate plus the exceed burst for the committed information rate or peak information rate.

If the conform action is set to **drop**, the exceed and violate actions are automatically set to **drop**. If the exceed action is set to **drop**, the violate action is automatically set to **drop**.

You can configure violate-action to send the packet unmodified, mark using explicit values, and use all combinations of enhanced packet marking. Enhanced packet marking modifies a QoS marking based on any incoming QoS marking and table maps. The switch also supports marking multiple QoS parameters for the same class and simultaneously configuring conform-action, exceed action, and violate-action marking.

Access policy-map class police configuration mode by entering the **police** policy-map class command. See the **police** command for more information.

You can use this command to set one or more violate actions for a traffic class.

For both individual and aggregate policers, if you do not configure a violate action, by default the violate class is assigned the same action as the exceed action.

**Examples**

This example shows how configure multiple actions in a policy map that sets an information rate of 23000 bits per second (b/s) and a burst rate of 10000 b/s:

```
Switch(config)# policy-map map1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police 23000 10000
Switch(config-pmap-c-police)# conform-action transmit
Switch(config-pmap-c-police)# exceed-action set-prec-transmit prec table
policed-prec-table-map-name
Switch(config-pmap-c-police)# violate-action drop
Switch(config-pmap-c-police)# exit
```

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

**Related Commands**

Command	Description
<b>class</b>	Defines a traffic classification match criteria for the specified class-map name.
<b>conform-action</b>	Defines the action to take on traffic that conforms to the CIR.
<b>exceed-action</b>	Defines the action to take on traffic between the conform rate and the conform rate plus the exceed burst.
<b>police</b>	Defines a policer for classified traffic.
<b>policy-map</b>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
<b>show policy-map</b>	Displays quality of service (QoS) policy maps.

# vlan

Use the **vlan** global configuration command with a VLAN ID to add a VLAN and to enter VLAN configuration mode. Use the **no** form of this command to delete the VLAN. Configuration information for normal-range VLANs (VLAN IDs 1 to 1005) is always saved in the VLAN database as well as in the switch running configuration file. Configuration information for extended-range VLANs (VLAN IDs greater than 1005), are saved only in the switch running configuration file. You can save configurations in the switch startup configuration file by entering the **copy running-config startup-config** privileged EXEC command.

**vlan** *vlan-id*

**no vlan** *vlan-id*

## Syntax Description

<i>vlan-id</i>	ID of the VLAN to be added and configured. For <i>vlan-id</i> , the range is 1 to 4094. You can enter a single VLAN ID, a series of VLAN IDs separated by commas, or a range of VLAN IDs separated by hyphens.
----------------	--

## Defaults

This command has no default settings.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

Extended-range VLANs (VLAN IDs 1006 to 4094) are not added to the VLAN database, but all VLAN configurations are saved in the running configuration, and you can save them in the switch startup configuration file.

Entering the **vlan** command with a VLAN ID enables VLAN configuration mode. If you enter an invalid VLAN ID, you receive an error message and do not enter 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 VLAN configuration mode. Only the **shutdown** command (for VLANs 1 to 1005) takes effect immediately.

These configuration commands are available in VLAN configuration mode. The **no** form of each command returns the characteristic to its default state.



### Note

Although all commands are visible, the only VLAN configuration commands that are supported on extended-range VLANs are **mtu** *mtu-size*, **private-vlan**, **remote-span** and **uni-vlan**. For extended-range VLANs, all other characteristics must remain at the default state.

**Note**

The switch supports only Ethernet VLANs. You can configure parameters for FDDI and Token Ring VLANs and view the results in the `vlan.dat` file, but these parameters are not used.

- **are** *are-number*: defines the maximum number of all-routes explorer (ARE) hops for TrCRF VLANs. The range is 0 to 13. The default is 7.
- **backupcrf** {**enable** | **disable**}: specifies the backup CRF mode for TrCRF VLANs.
- **bridge** {*bridge-number* | **type**}: specifies the logical distributed source-routing bridge, the bridge that interconnects all logical rings having this VLAN as a parent VLAN in FDDI-NET, Token Ring-NET, and TrBRF VLANs. The range is 0 to 15. The default bridge number is 0.
- **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.
  - **ethernet** is Ethernet media type (the default).
  - **fddi** is FDDI media type.
  - **fd-net** is FDDI network entity title (NET) media type.
  - **tokenring** is Token Ring media type or TrCRF.
  - **tr-net** is Token Ring network entity title (NET) media type or TrBRF media type.
- **mtu** *mtu-size*: specifies the maximum transmission unit (MTU) (packet size in bytes). The range is 1500 to 18190. The default is 1500 bytes.
- **name** *vlan-name*: names the VLAN with an ASCII string from 1 to 32 characters that must be unique within the administrative domain. The default is `VLANxxxx` where `xxxx` represents four numeric digits (including leading zeros) equal to the VLAN ID number.
- **no**: negates a command or returns it to the default setting.
- **parent** *parent-vlan-id*: specifies the parent VLAN of an existing FDDI, Token Ring, or TrCRF VLAN. The range is 0 to 1005. The default parent VLAN ID is 0 (no parent VLAN).
- **private-vlan**: configure the VLAN as a private VLAN community, isolated, or primary VLAN or configure the association between private-VLAN primary and secondary VLANs. See the [private-vlan](#) command for more information.
- **remote-span**: configure the VLAN as a Remote SPAN (RSPAN) VLAN. When the RSPAN feature is added to an existing VLAN, the VLAN is first deleted and is then recreated with the RSPAN feature. Any access ports are deactivated until the RSPAN feature is removed. Learning is disabled on the VLAN. See the [remote-span](#) command for more information.
- **ring** *ring-number*: defines the logical ring for an FDDI, Token Ring, or TrCRF VLAN. The range is 1 to 4095.
- **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 for 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.
  - **ieee** for IEEE Ethernet STP running source-route transparent (SRT) bridging.
  - **ibm** for IBM STP running source-route bridging (SRB).
  - **auto** for STP running a combination of source-route transparent bridging (IEEE) and source-route bridging (IBM).
- **tb-vlan1** *tb-vlan1-id* and **tb-vlan2** *tb-vlan2-id*: specifies the first and second VLAN to which this VLAN is translationally bridged. Translational VLANs translate FDDI or Token Ring to Ethernet, for example. The range is 0 to 1005. If no value is specified, 0 (no transitional bridging) is assumed.
- **uni-vlan {community | isolated}**: configures the VLAN as a user network interface-enhanced network interface (UNI-ENI) community or UNI-ENI isolated VLAN. UNIs on a switch that are assigned to a community VLAN can communicate with each other. If the UNI-ENI VLAN is isolated (the default), ports in the VLAN cannot communicate. See the **uni count** command for more information.

## Examples

This example shows how to add an Ethernet VLAN with default media characteristics. The default includes a *vlan-name* of *VLANxxx*, where *xxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number. The default **media** option is **ethernet**; the **state** option is **active**. The default *said-value* variable is 100000 plus the VLAN ID; the *mtu-size* variable is 1500; the **stp-type** option is **ieee**. When you enter the **exit** VLAN configuration command, the VLAN is added if it did not already exist; otherwise, this command does not have any effect.

This example shows how to create a new VLAN with all default characteristics and enter config-vlan mode:

```
Switch(config)# vlan 200
Switch(config-vlan)# exit
```

This example shows how to create a new extended-range VLAN, to enter VLAN configuration mode and configure the VLAN as a UNI-ENI community VLAN, and to save the new VLAN in the switch startup configuration file:

```
Switch(config)# vlan 2000
Switch(config-vlan)# uni-vlan community
Switch(config-vlan)# exit
Switch(config)# exit
Switch# copy running-config startup config
```

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

## Related Commands

Command	Description
<a href="#">show vlan</a>	Displays the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified).

## vlan access-map

Use the **vlan access-map** global configuration command to create or modify a VLAN map entry for VLAN packet filtering. This entry changes the mode to the VLAN access-map configuration. Use the **no** form of this command to delete a VLAN map entry. Use the **vlan filter** interface configuration command to apply a VLAN map to one or more VLANs.

**vlan access-map** *name* [*number*]

**no vlan access-map** *name* [*number*]

### Syntax Description

<i>name</i>	Name of the VLAN map.
<i>number</i>	(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.

### Defaults

There are no VLAN map entries and no VLAN maps applied to a VLAN.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(44)EY	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.

In global configuration mode, use the **vlan filter** interface configuration command to apply the map to one or more VLANs.

**Note**

For more information about VLAN map entries, see the software configuration guide for this release.

**Examples**

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.

```
Switch(config)# vlan access-map vac1
Switch(config-access-map)# match ip address acl1
Switch(config-access-map)# action forward
```

This example shows how to delete VLAN map *vac1*:

```
Switch(config)# no vlan access-map vac1
```

**Related Commands**

Command	Description
<a href="#">action</a>	Sets the action for the VLAN access map entry.
<a href="#">match (access-map configuration)</a>	Sets the VLAN map to match packets against one or more access lists.
<a href="#">show vlan access-map</a>	Displays information about a particular VLAN access map or all VLAN access maps.
<a href="#">vlan filter</a>	Applies the VLAN access map to one or more VLANs.

# vlan dot1q tag native

Use the **vlan dot1q tag native** global configuration command to enable tagging of native VLAN frames on all IEEE 802.1Q trunk ports. Use the **no** form of this command to return to the default setting.

**vlan dot1q tag native**

**no vlan dot1q tag native**

This command is supported only when the metro access or metro IP access image is running on the switch.

**Syntax Description** This command has no arguments or keywords.

**Defaults** IEEE 802.1Q native VLAN tagging is disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** When enabled, native VLAN packets going out all 802.1Q trunk ports are tagged. When disabled, native VLAN packets going out all 802.1Q trunk ports are not tagged.

You can use this command with the 802.1Q tunneling feature. This feature operates on an edge switch of a service-provider network and expands VLAN space by using a VLAN-in-VLAN hierarchy and tagging the tagged packets. You must use 802.1Q trunk ports for sending packets to the service-provider network. However, packets going through the core of the service-provider network might also be carried on 802.1Q trunks. If the native VLANs of an 802.1Q trunks match the native VLAN of a tunneling port on the same switch, traffic on the native VLAN is not tagged on the sending trunk port. This command ensures that native VLAN packets on all 802.1Q trunk ports are tagged.



**Note**

For more information about 802.1Q tunneling, see the software configuration guide for this release.

**Examples** This example shows how to enable 802.1Q tagging on native VLAN frames:

```
Switch# configure terminal
Switch (config)# vlan dot1q tag native
Switch (config)# end
```

You can verify your settings by entering the **show vlan dot1q tag native** privileged EXEC command.



Related Commands	Command	Description
	<code>show vlan dot1q tag native</code>	Displays 802.1Q native VLAN tagging status.

# vlan filter

Use the **vlan filter** global configuration command to apply a VLAN map to one or more VLANs. Use the **no** form of this command to remove the map.

```
vlan filter mapname vlan-list {list | all}
```

```
no vlan filter mapname vlan-list {list | all}
```

## Syntax Description

<i>mapname</i>	Name of the VLAN map entry.
<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.
<b>all</b>	Remove the filter from all VLANs.

## Defaults

There are no VLAN filters.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EY	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.



### Note

For more information about VLAN map entries, see the software configuration guide for this release.

## Examples

This example applies VLAN map entry *map1* to VLANs 20 and 30:

```
Switch(config)# vlan filter map1 vlan-list 20, 30
```

This example shows how to delete VLAN map entry *map1* from VLAN 20:

```
Switch(config)# no vlan filter map1 vlan-list 20
```

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

Related Commands	Command	Description
	<a href="#">show vlan access-map</a>	Displays information about a particular VLAN access map or all VLAN access maps.
	<a href="#">show vlan filter</a>	Displays information about all VLAN filters or about a particular VLAN or VLAN access map.
	<a href="#">vlan access-map</a>	Creates a VLAN map entry for VLAN packet filtering.

## vmps reconfirm (privileged EXEC)

Use the **vmps reconfirm** privileged EXEC command to immediately send VLAN Query Protocol (VQP) queries to reconfirm all dynamic VLAN assignments with the VLAN Membership Policy Server (VMPS).

### vmps reconfirm

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default is defined.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Examples** This example shows how to immediately send VQP queries to the VMPS:

```
Switch# vmps reconfirm
```

You can verify your setting by entering the **show vmps** privileged EXEC command and examining the VMPS Action row of the Reconfirmation Status section. The **show vmps** command shows the result of the last time the assignments were reconfirmed either because the reconfirmation timer expired or because the **vmps reconfirm** command was entered.

Related Commands	Command	Description
	<a href="#">show vmps</a>	Displays VQP and VMPS information.
	<a href="#">vmps reconfirm (global configuration)</a>	Changes the reconfirmation interval for the VQP client.

## vmpls reconfirm (global configuration)

Use the **vmpls reconfirm** global configuration command to change the reconfirmation interval for the VLAN Query Protocol (VQP) client. Use the **no** form of this command to return to the default setting.

**vmpls reconfirm** *interval*

**no vmpls reconfirm**

<b>Syntax Description</b>	<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.
---------------------------	-----------------	--

**Defaults** The default reconfirmation interval is 60 minutes.

**Command Modes** Global configuration

### Command History

**Examples** This example shows how to set the VQP client to reconfirm dynamic VLAN entries every 20 minutes:

```
Switch(config)# vmpls reconfirm 20
```

You can verify your setting by entering the **show vmpls** privileged EXEC command and examining information in the Reconfirm Interval row.

Related Commands	Command	Description
	<a href="#">show vmpls</a>	Displays VQP and VMPS information.
	<a href="#">vmpls reconfirm (privileged EXEC)</a>	Sends VQP queries to reconfirm all dynamic VLAN assignments with the VMPS.

## vmps retry

Use the **vmps retry** global configuration command to configure the per-server retry count for the VLAN Query Protocol (VQP) client. Use the **no** form of this command to return to the default setting.

**vmps retry** *count*

**no vmps retry**

<b>Syntax Description</b>	<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.
---------------------------	--------------	---

<b>Defaults</b>	The default retry count is 3.
-----------------	-------------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

**Examples** This example shows how to set the retry count to 7:

```
Switch(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.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show vmps</a>	Displays VQP and VMPS information.

## vmmps server

Use the **vmmps server** global configuration command to configure the primary VLAN Membership Policy Server (VMPS) and up to three secondary servers. Use the **no** form of this command to remove a VMPS server.

```
vmmps server ipaddress [primary]
```

```
no vmmps server [ipaddress]
```

Syntax Description	
<i>ipaddress</i>	IP address or hostname of the primary or secondary VMPS servers. If you specify a hostname, the Domain Name System (DNS) server must be configured.
<b>primary</b>	(Optional) Decides whether primary or secondary VMPS servers are being configured.

**Defaults** No primary or secondary VMPS servers are defined.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(44)EY	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.

When using the **no** form without specifying the *ipaddress*, all configured servers are deleted. If you delete all servers when dynamic-access ports are present, the switch cannot forward packets from new sources on these ports because it cannot query the VMPS.

**Examples** This example shows how to configure the server that has 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:

```
Switch(config)# vmmps server 191.10.49.20 primary
Switch(config)# vmmps server 191.10.49.21
Switch(config)# vmmps server 191.10.49.22
```

This example shows how to delete the server with IP address 191.10.49.21:

```
Switch(config)# no vmmps server 191.10.49.21
```

You can verify your setting by entering the **show vmmps** privileged EXEC command and examining information in the VMPS Domain Server row.

■ vmps server

Related Commands	Command	Description
	<a href="#">show vmps</a>	Displays VQP and VMPS information.



# vrf upgrade-cli multi-af-mode

To reconfigure the IPv4 VPN routing and forwarding (VRF) commands to allow IPv6 multi-address family VRF support for configured IPv4 VRFs, use the **vrf upgrade-cli multi-af-mode in** global configuration mode.

```
vrf upgrade-cli multi-af-mode {common-policies | non-common-policies} [vrf name] [force]
```



## Note

To use this command the switch must be running the metro IP access image.

## Syntax Description

<b>common-policies</b>	Specifies that all IPv4 VRF policies are common IPv4 and IPv6 VRF policies.
<b>non-common-policies</b>	Specifies that IPv4 VRF policies are not common VRF policies, but remain as IPv4-only VRF policies.
<b>vrf name</b>	(Optional) Specifies a particular VRF to migrate or not migrate to IPv6 format by entering the VRF name.
<b>force</b>	(Optional) Specifies that the switch not prompt for confirmation for the configuration.

## Defaults

IPv4 policies are not supported for IPv6

## Command Modes

Global configuration

## Command History

Release	Modification
12.2.(58)SE	This command was introduced.

## Usage Guidelines

This command lets you migrate existing IPv4 VRFs for multi-address family IPv4 and IPv6 VRF support. When you use IPv4 commands to configure a VRF, they only apply to IPv4 traffic. When you use the **vrf definition** *vrf-name* global configuration command to enter VRF configuration mode, followed by the **address-family** commands, if you include both IPv4 and IPv6 address families, the configuration applies to both IPv4 and IPv6 traffic.

When you enter this command, IPv4 VRFs that are already configured also allow IPv6 traffic after you enter the **address-family ipv6** command.

Because this command is used only one time, there is not a **no** version of the command.

This command is not stored in NVRAM because it has a one-time, immediate effect.

To configure IPv6 VRF-aware routing, you must use the **dual-ipv4-and-ipv6 routing** template or the **dual-ipv4-and-ipv6 default** template. The **dual-ipv4-and-ipv6 vlan** template does not support VRF-aware routing.

**Examples**

This example shows how to configure the switch to migrate all existing IPv4 VRF CLI to the CLI that supports IPv4 and IPv6 VRF.

```
Switch(config)# vrf upgrade-cli multi-af-mode common-policies
```

This example shows how to configure the switch to migrate only the VRF named *test* to the CLI that supports IPv4 and IPv6 traffic. All other IPv4 VRFs are not modified.

```
Switch(config)# vrf upgrade-cli multi-af-mode non-common-policies vrf test
```

**Related Commands**

Command	Description
<b>address-family ipv4</b>	Configures a routing session using standard IPv4 address prefixes.
<b>address-family ipv6</b>	configures a routing session using standard IPv6 address prefixes
<b>vrf definition</b> <i>vrf-name</i>	Configures a VPN VRF routing table and enters VRF configuration mode.
<b>vrf forwarding</b> <i>vrf-name</i>	Associates a Virtual Routing and Forwarding (VRF) instance or a virtual network with an interface.



## APPENDIX **A**

# Cisco ME 3400E Ethernet Access Switch Boot Loader Commands

---

This appendix describes the boot loader commands on the Cisco ME 3400 Ethernet Access switch. During normal boot loader operation, you are not presented with the boot loader command-line prompt. You gain access to the boot loader command line if the switch is set to manually boot, if an error occurs during power-on self-test (POST) DRAM testing, or if an error occurs while loading the operating system (a corrupted Cisco IOS image). You can also access the boot loader if you have lost or forgotten the switch password.



### Note

The default switch configuration allows an end user with physical access to the switch to recover from a lost password by interrupting the boot process while the switch is powering up and then entering a new password. The password recovery disable feature allows the system administrator to protect access to the switch password by disabling part of this functionality and allowing the user to interrupt the boot process only by agreeing to set the system back to the default configuration. With password recovery disabled, the user can still interrupt the boot process and change the password, but the configuration file (config.text) and the VLAN database file (vlan.dat) are deleted. For more information, see the software configuration guide for this release.

---

You can access the boot loader through a switch console connection at 9600 bps. Disconnect and then reconnect the switch power cord. After the switch performs POST, the switch begins the autoboot process. The boot loader prompts the user for a break key character during the boot-up sequence, as shown in this example:

```
***** The system will autoboot in 15 seconds *****
```

```
Send a break key to prevent autobooting.
```

The break key character is different for each operating system.

- On a SUN work station running UNIX, Ctrl-C is the break key.
- On a PC running Windows 2000, Ctrl-Break is the break key.

Cisco TAC has tabulated break keys for most common operating systems and has provided an alternative break key sequence for terminal emulators that do not support the break keys. To view this table, see:

<http://www.cisco.com/warp/public/701/61.html#how-to>

When you enter the break key, the boot loader *switch:* prompt appears.

The boot loader performs low-level CPU initialization, performs POST, and loads a default operating system image into memory.

# arp

Use the **arp** boot loader command to display the contents the Address Resolution Protocol (ARP) table.

**arp** [*ip\_address*]

<b>Syntax Description</b>	<i>ip_address</i> (Optional) Show the ARP table or the mapping for a specific IP address.
---------------------------	---

<b>Command Modes</b>	Boot loader
----------------------	-------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

<b>Usage Guidelines</b>	The ARP table has the IP-address-to-MAC-address mappings.
-------------------------	---

<b>Examples</b>	This example shows how to display the ARP table:
-----------------	--

```
switch: arp 172.20.136.8
arp'ing 172.20.136.8...
172.20.136.8 is at 00:1b:78:d1:25:ae, via port 0
```

# boot

Use the **boot** boot loader command to load and boot an executable image and to enter the command-line interface.

```
boot [-post | -n | -p | flag] filesystem:!file-url ...
```

## Syntax Description

<b>-post</b>	(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.
<b>-n</b>	(Optional) Pause for the Cisco IOS debugger immediately after launching.
<b>-p</b>	(Optional) Pause for the JTAG debugger right after loading the image.
<i>filesystem</i> :	Alias for a flash file system. Use <b>flash</b> : for the system board flash device.
<i>!file-url</i>	(Optional) Path (directory) and name of a bootable image. Separate image names with a semicolon.

## Defaults

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

## Command Modes

Boot loader

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

When you enter the **boot** command without any arguments, the switch attempts to automatically boot the system by using the information in the BOOT environment variable, if any. If you supply an image name for the *file-url* variable, the **boot** command attempts to boot the specified image.

When you set boot loader **boot** command options, they are executed immediately and apply only to the current boot loader session. These settings are not saved for the next boot operation.

Filenames and directory names are case sensitive.

## Examples

This example shows how to boot the switch using the *new-image.bin* image:

```
switch: boot flash:/new-images/new-image.bin
```

After entering this command, you are prompted to start the setup program.

Related Commands	Command	Description
	<a href="#">set</a>	Sets the BOOT environment variable to boot a specific image when the <b>BOOT</b> keyword is appended to the command.

# cat

Use the **cat** boot loader command to display the contents of one or more files.

```
cat filesystem:/file-url ...
```

Syntax Description	
<i>filesystem:</i>	Alias for a flash file system. Use <b>flash:</b> for the system board flash device.
<i>/file-url</i>	Path (directory) and name of the files to display. Separate each filename with a space.

Command Modes	
	Boot loader

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

Usage Guidelines	
	Filenames and directory names are case sensitive.
	If you specify a list of files, the contents of each file appears sequentially.

Examples	
	This example shows how to display the contents of two files:

```
switch: cat flash:/new-images/info flash:env_vars
version_suffix: image-name
version_directory: image-name
image_name: image-name.bin
ios_image_file_size: 63984644
total_image_file_size: 8133632
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: me340x
info_end:
BAUD=57600
MANUAL_BOOT=no
```

Related Commands	Command	Description
	<a href="#">more</a>	Displays the contents of one or more files.
	<a href="#">type</a>	Displays the contents of one or more files.

# copy

Use the **copy** boot loader command to copy a file from a source to a destination.

```
copy [-b block-size] filesystem:/source-file-url filesystem:/destination-file-url
```

Syntax Description		
<b>-b</b> <i>block-size</i>	(Optional)	This option is used only for internal development and testing.
<i>filesystem:</i>	Alias for a flash file system. Use <b>flash:</b> for the system board flash device.	
<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.	

**Defaults** The default block size is 4 KB.

**Command Modes** Boot loader

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines**

Filename and directory names are case sensitive.

Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Filename is limited to 45 characters; the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

If you are copying a file to a new directory, the directory must already exist.

**Examples**

This example shows how to copy a file at the root:

```
switch: copy flash:test1.text flash:test4.text
.
```

File "flash:test1.text" successfully copied to "flash:test4.text"

You can verify that the file was copied by entering the **dir** *filesystem:* boot loader command.

Related Commands	Command	Description
	<a href="#">delete</a>	Deletes one or more files from the specified file system.



# delete

Use the **delete** boot loader command to delete one or more files from the specified file system.

```
delete filesystem:/file-url ...
```

Syntax Description	
<i>filesystem:</i>	Alias for a flash file system. Use <b>flash:</b> for the system board flash device.
<i>/file-url</i>	Path (directory) and filename to delete. Separate each filename with a space.

Command Modes	Boot loader
---------------	-------------

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

Usage Guidelines	<p>Filenames and directory names are case sensitive.</p> <p>The switch prompts you for confirmation before deleting each file.</p>
------------------	--

Examples	<p>This example shows how to delete two files:</p> <pre><b>switch: delete flash:test2.text flash:test5.text</b> Are you sure you want to delete "flash:test2.text" (y/n)?y File "flash:test2.text" deleted Are you sure you want to delete "flash:test5.text" (y/n)?y File "flash:test2.text" deleted</pre>
----------	---

You can verify that the files were deleted by entering the **dir flash:** boot loader command.

Related Commands	Command	Description
	<a href="#">copy</a>	Copies a file from a source to a destination.

# dir

Use the **dir** boot loader command to display a list of files and directories on the specified file system.

**dir** *filesystem:/file-url ...*

Syntax Description	
<i>filesystem:</i>	Alias for a flash file system. Use <b>flash:</b> for the system board flash device.
<i>/file-url</i>	(Optional) Path (directory) and directory name whose contents you want to display. Separate each directory name with a space.

Command Modes	Boot loader
---------------	-------------

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

Usage Guidelines	Directory names are case sensitive.
------------------	-------------------------------------

Examples	This example shows how to display the files in flash memory:
----------	--

```
switch: dir flash:
```

```
Directory of flash:/
```

```

  3  -rwx      1839   Mar 01 2002 00:48:15  config.text
 11  -rwx      1140   Mar 01 2002 04:18:48   vlan.dat
 21  -rwx         26   Mar 01 2002 00:01:39   env_vars
  9  drwx       768   Mar 01 2002 23:11:42   html
 16  -rwx      1037   Mar 01 2002 00:01:11   config.text
 14  -rwx      1099   Mar 01 2002 01:14:05   homepage.htm
 22  -rwx         96   Mar 01 2002 00:01:39   system_env_vars
 17  drwx       192   Mar 06 2002 23:22:03   image-name
```

```
15998976 bytes total (6397440 bytes free)
```

[Table A-1](#) describes the fields in the display.

**Table A-1** *dir* Field Descriptions

Field	Description
2	Index number of the file.
-rwx	File permission, which can be any or all of the following: <ul style="list-style-type: none"> <li>• d—directory</li> <li>• r—readable</li> <li>• w—writable</li> <li>• x—executable</li> </ul>
1644045	Size of the file.
<date>	Last modification date.
env_vars	Filename.

**Related Commands**

Command	Description
<a href="#">mkdir</a>	Creates one or more directories.
<a href="#">rmdir</a>	Removes one or more directories.

# flash\_init

Use the **flash\_init** boot loader command to initialize the flash file system.

**flash\_init**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** The flash file system is automatically initialized during normal system operation.

---

**Command Modes** Boot loader

---

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

---



---


**Usage Guidelines** During the normal boot process, the flash file system is automatically initialized.

Use this command to manually initialize the flash file system. For example, you use this command during the recovery procedure for a lost or forgotten password.

# format

Use the **format** boot loader command to format the specified file system and destroy all data in that file system.

**format** *filesystem:*

<b>Syntax Description</b>	<i>filesystem:</i>	Alias for a flash file system. Use <b>flash:</b> for the system board flash device.
<b>Command Modes</b>	Boot loader	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.
<b>Usage Guidelines</b>		
 <b>Caution</b>	Use this command with care; it destroys all data on the file system and renders your system unusable.	

# fsck

Use the **fsck** boot loader command to check the file system for consistency.

**fsck** [-test | -f] *filesystem*:

Syntax Description		
	<b>-test</b>	(Optional) Initialize the file system code and perform extra POST on flash memory. An extensive, nondestructive memory test is performed on every byte that makes up the file system.
	<b>-f</b>	(Optional) Initialize the file system code and perform a fast file consistency check. Cyclic redundancy checks (CRCs) in the flashfs sectors are not checked.
	<i>filesystem</i> :	Alias for a flash file system. Use <b>flash:</b> for the system board flash device.

**Defaults** No file system check is performed.

**Command Modes** Boot loader

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** To stop an in-progress file system consistency check, disconnect the switch power and then reconnect the power.

**Examples** This example shows how to perform an extensive file system check on flash memory:

```
switch: fsck -test flash:
```

# help

Use the **help** boot loader command to display the available commands.

**help**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Modes** Boot loader

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

---

---

**Usage Guidelines** You can also use the question mark (?) to display a list of available boot loader commands.

# memory

Use the **memory** boot loader command to display memory heap utilization information.

## memory

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Boot loader

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Examples** This example shows how to display memory heap utilization information:

```
switch: memory
Text:    0x00700000 - 0x0071cf24 (0x0001cf24 bytes)
Rotext:  0x00000000 - 0x00000000 (0x00000000 bytes)
Data:    0x0071cf24 - 0x00723a0c (0x00006ae8 bytes)
Bss:     0x0072529c - 0x00746f94 (0x00021cf8 bytes)
Heap:    0x00756f98 - 0x00800000 (0x000a9068 bytes)
```

Bottom heap utilization is 22 percent.

Top heap utilization is 0 percent.

Total heap utilization is 22 percent.

Total bytes: 0xa9068 (692328)

Bytes used: 0x26888 (157832)

Bytes available: 0x827e0 (534496)

Alternate heap utilization is 0 percent.

Total alternate heap bytes: 0x6fd000 (7327744)

Alternate heap bytes used: 0x0 (0)

Alternate heap bytes available: 0x6fd000 (7327744)

[Table A-2](#) describes the fields in the display.

**Table A-2** *memory Field Descriptions*

Field	Description
Text	Beginning and ending address of the text storage area.
Rotext	Beginning and ending address of the read-only text storage area. This part of the data segment is grouped with the Text entry.
Data	Beginning and ending address of the data segment storage area.
Bss	Beginning and ending address of the block started by symbol (Bss) storage area. It is initialized to zero.
Heap	Beginning and ending address of the area in memory that memory is dynamically allocated to and freed from.



# mgmt\_clr

Use the **mgmt\_clr** boot loader command to clear the Ethernet management port statistics.

**mgmt\_clr**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Modes** Boot loader

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

---

---

**Examples** This example shows how to clear the Ethernet management port statistics:

```
switch: mgmt_clr
```

# mgmt\_init

Use the **mgmt\_init** boot loader command to initialize the Ethernet management port.

**mgmt\_init**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Modes** Boot loader

---

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

---



---

**Usage Guidelines** Use the **mgmt\_init** command only during debugging of the Ethernet management port.

---

**Examples** This example shows how to initialize the Ethernet management port:

```
switch: mgmt_init
```

# mgmt\_show

Use the **mgmt\_show** boot loader command to display the Ethernet management port statistics.

**mgmt\_show**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Boot loader

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Examples** This example shows how to display the Ethernet management port statistics:

```
switch: mgmt_show
Statistics                Received      Transmitted
-----
good frame bytes         :           60          120
good frames               :            1            2
bad frames                :            0            0
dropped frames           :            0            0
queue overflowed         :            0            0
memory access errors     :            0            0
```

# mkdir

Use the **mkdir** boot loader command to create one or more new directories on the specified file system.

**mkdir** *filesystem:/directory-url ...*

Syntax Description	<i>filesystem:</i>	Alias for a flash file system. Use <b>flash:</b> for the system board flash device.
	<i>/directory-url</i>	Name of the directories to create. Separate each directory name with a space.

Command Modes	Boot loader
---------------	-------------

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

Usage Guidelines	Directory names are case sensitive.
	Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

**Examples** This example shows how to make a directory called Saved\_Configs:

```
switch: mkdir flash:Saved_Configs
Directory "flash:Saved_Configs" created
```

This example shows how to make two directories:

```
switch: mkdir flash:Saved_Configs1 flash:Test
Directory "flash:Saved_Configs1" created
Directory "flash:Test" created
```

You can verify that the directory was created by entering the **dir** *filesystem:* boot loader command.

Related Commands	Command	Description
	<a href="#">dir</a>	Displays a list of files and directories on the specified file system.
	<a href="#">rmdir</a>	Removes one or more directories from the specified file system.

# more

Use the **more** boot loader command to display the contents of one or more files.

```
more filesystem:/file-url ...
```

Syntax Description	
<i>filesystem:</i>	Alias for a flash file system. Use <b>flash:</b> for the system board flash device.
<i>/file-url</i>	Path (directory) and name of the files to display. Separate each filename with a space.

Command Modes	
	Boot loader

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

Usage Guidelines	
	Filenames and directory names are case sensitive.
	If you specify a list of files, the contents of each file appears sequentially.

Examples	
	This example shows how to display the contents of two files:

```
switch: more flash:/new-images/info flash:env_vars
version_suffix: image-name
version_directory: image-name
image_name: image-name.bin
ios_image_file_size: 63984644
total_image_file_size: 8133632
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
info_end:
BAUD=57600
MANUAL_BOOT=no
```

Related Commands	Command	Description
	<a href="#">cat</a>	Displays the contents of one or more files.
	<a href="#">type</a>	Displays the contents of one or more files.

# rename

Use the **rename** boot loader command to rename a file.

```
rename filesystem:/source-file-url filesystem:/destination-file-url
```

Syntax Description	
<i>filesystem:</i>	Alias for a flash file system. Use <b>flash:</b> for the system board flash device.
<i>/source-file-url</i>	Original path (directory) and filename.
<i>/destination-file-url</i>	New path (directory) and filename.

Command Modes	
	Boot loader

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

Usage Guidelines	
	<p>Filenames and directory names are case sensitive.</p> <p>Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.</p> <p>Filenames are limited to 45 characters; the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.</p>

Examples	
	<p>This example shows a file named <i>config.text</i> being renamed to <i>config1.text</i>:</p>

```
switch: rename flash:config.text flash:config1.text
```

You can verify that the file was renamed by entering the **dir filesystem:** boot loader command.

Related Commands	Command	Description
	<a href="#">copy</a>	Copies a file from a source to a destination.

# reset

Use the **reset** boot loader command to perform a hard reset on the system. A hard reset is similar to power-cycling the switch, clearing the processor, registers, and memory.

**reset**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Modes** Boot loader

---

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

---

---

**Examples** This example shows how to reset the system:

```
switch: reset
Are you sure you want to reset the system (y/n)?y
System resetting...
```

---

Related Commands	Command	Description
	<a href="#">boot</a>	Loads and boots an executable image and enters the command-line interface.

---

# rmdir

Use the **rmdir** boot loader command to remove one or more empty directories from the specified file system.

```
rmdir filesystem:/directory-url ...
```

Syntax Description		
<i>filesystem:</i>	Alias for a flash file system. Use <b>flash:</b> for the system board flash device.	
<i>/directory-url</i>	Path (directory) and name of the empty directories to remove. Separate each directory name with a space.	

Command Modes	Boot loader
---------------	-------------

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines**

Directory names are case sensitive and limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Before removing a directory, you must first delete all the files in the directory.

The switch prompts you for confirmation before deleting each directory.

**Examples**

This example shows how to remove a directory:

```
switch: rmdir flash:Test
```

You can verify that the directory was deleted by entering the **dir** *filesystem:* boot loader command.

Related Commands	Command	Description
	<b>dir</b>	Displays a list of files and directories on the specified file system.
	<b>mkdir</b>	Creates one or more new directories on the specified file system.



# set

Use the **set** boot loader command to set or display environment variables, which can be used to control the boot loader or any other software running on the switch.

**set** *variable value*



## Note

Under normal circumstances, it is not necessary to alter the setting of the environment variables.

## Syntax Description

<i>variable value</i>	<p>Use one of these keywords for <i>variable and value</i>:</p> <p><b>MANUAL_BOOT</b>—Decides whether the switch automatically or manually boots. Valid values are 1, yes, 0, and no. If it is set to no or 0, the boot loader attempts to automatically boot the system. If it is set to anything else, you must manually boot the switch from the boot loader mode.</p> <p><b>BOOT filesystem:/file-url</b>—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> <p><b>ENABLE_BREAK</b>—Decides whether the automatic boot process can be interrupted by using the Break key on the console.</p> <p>Valid values are 1, yes, on, 0, no, and off. If it is set to 1, yes, or on, you can interrupt the automatic boot process by pressing the Break key on the console after the flash file system has initialized.</p> <p><b>HELPER filesystem:/file-url</b>—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> <p><b>PS1 prompt</b>—A string that is used as the command-line prompt in boot loader mode.</p> <p><b>CONFIG_FILE flash:/file-url</b>—The filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.</p> <p><b>BAUD rate</b>—The rate in bits per second (bps) used for the console. The Cisco IOS software inherits the baud rate setting from the boot loader and continues to use this value unless the configuration file specifies another setting. The range is from 0 to 4294967295 bps. 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> <p><b>HELPER_CONFIG_FILE filesystem:/file-url</b>—The name of the configuration file to be used by the Cisco IOS helper image. If this is not set, the file specified by the CONFIG_FILE environment variable is used by all versions of Cisco IOS that are loaded, including the helper image. This variable is used only for internal development and testing.</p>
-----------------------	---

**Defaults**

The environment variables have these default values:

MANUAL\_BOOT: No (0)

BOOT: Null string

ENABLE\_BREAK: No (Off or 0) (the automatic boot process cannot be interrupted by pressing the Break key on the console).

HELPER: No default value (helper files are not automatically loaded).

PS1: switch:

CONFIG\_FILE: config.text

BAUD: 9600 bps

HELPER\_CONFIG\_FILE: No default value (no helper configuration file is specified).

SWITCH\_NUMBER: 1

SWITCH\_PRIORITY: 1

**Note**

Environment variables that have values are stored in the flash file system in various files. The format of these files is that each line contains an environment variable name and an equal sign followed by the value of the variable. A variable has no value if it is not listed in this file; it has a value if it is listed in the file even if the value is a null string. A variable that is set to a null string (for example, “ ”) is a variable with a value. Many environment variables are predefined and have default values.

**Command Modes**

Boot loader

**Command History**

Release	Modification
12.2(44)EY	This command was introduced.

Environment variables are case sensitive and must be entered as documented.

Environment variables that have values are stored in flash memory outside of the flash file system.

Under normal circumstances, it is not necessary to alter the setting of the environmental variables.

The MANUAL\_BOOT environment variable can also be set by using the **boot manual** global configuration command.

The BOOT environment variable can also be set by using the **boot system filesystem:/file-url** global configuration command.

The ENABLE\_BREAK environment variable can also be set by using the **boot enable-break** global configuration command.

The HELPER environment variable can also be set by using the **boot helper filesystem:/file-url** global configuration command.

The CONFIG\_FILE environment variable can also be set by using the **boot config-file flash:/file-url** global configuration command.

The HELPER\_CONFIG\_FILE environment variable can also be set by using the **boot helper-config-file filesystem:/file-url** global configuration command.

The HELPER\_CONFIG\_FILE environment variable can also be set by using the **boot helper-config-file filesystem:/file-url** global configuration command.

The boot loader prompt string (PS1) can be up to 120 printable characters except the equal sign (=).

---

**Examples**

This example shows how to change the boot loader prompt:

```
switch: set PS1 loader:  
loader:
```

You can verify your setting by using the **set** boot loader command.

---

**Related Commands**

Command	Description
<a href="#">unset</a>	Resets one or more environment variables to its previous setting.

# type

Use the **type** boot loader command to display the contents of one or more files.

**type** *filesystem:/file-url ...*

Syntax Description	
<i>filesystem:</i>	Alias for a flash file system. Use <b>flash:</b> for the system board flash device.
<i>/file-url</i>	Path (directory) and name of the files to display. Separate each filename with a space.

Command Modes	
	Boot loader

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

Usage Guidelines	
	<p>Filenames and directory names are case sensitive.</p> <p>If you specify a list of files, the contents of each file appears sequentially.</p>

Examples	
	<p>This example shows how to display the contents of two files:</p>

```
switch: type flash:/new-images/info flash:env_vars
version_suffix: image-name
version_directory: image-name
image_name: image-name.bin
ios_image_file_size: 63984644
total_image_file_size: 8133632
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
info_end:
BAUD=57600
MANUAL_BOOT=no
```

Related Commands	Command	Description
	<b>cat</b>	Displays the contents of one or more files.
	<b>more</b>	Displays the contents of one or more files.

# unset

Use the **unset** boot loader command to reset one or more environment variables.

**unset** *variable* ...



## Note

Under normal circumstances, it is not necessary to alter the setting of the environment variables.

## Syntax Description

*variable*

Use one of these keywords for *variable*:

**MANUAL\_BOOT**—Decides whether the switch automatically or manually boots.

**BOOT**—Resets the list of executable files to try to load and execute when automatically booting. If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash file system. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash file system.

**ENABLE\_BREAK**—Decides whether the automatic boot process can be interrupted by using the Break key on the console after the flash file system has been initialized.

**HELPER**—A semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.

**PS1**—A string that is used as the command-line prompt in boot loader mode.

**CONFIG\_FILE**—Resets the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.

**BAUD**—Resets the rate in bits per second (bps) used for the console. The Cisco IOS software inherits the baud rate setting from the boot loader and continues to use this value unless the configuration file specifies another setting.

**HELPER\_CONFIG\_FILE**—Resets the name of the configuration file to be used by the Cisco IOS helper image. If this is not set, the file specified by the CONFIG\_FILE environment variable is used by all versions of Cisco IOS that are loaded, including the helper image. This variable is used only for internal development and testing.

## Command Modes

Boot loader

## Command History

### Release

### Modification

12.2(44)EY

This command was introduced.

**Usage Guidelines**

Under normal circumstances, it is not necessary to alter the setting of the environmental variables.

The MANUAL\_BOOT environment variable can also be reset by using the **no boot manual** global configuration command.

The BOOT environment variable can also be reset by using the **no boot system** global configuration command.

The ENABLE\_BREAK environment variable can also be reset by using the **no boot enable-break** global configuration command.

The HELPER environment variable can also be reset by using the **no boot helper** global configuration command.

The CONFIG\_FILE environment variable can also be reset by using the **no boot config-file** global configuration command.

The HELPER\_CONFIG\_FILE environment variable can also be reset by using the **no boot helper-config-file** global configuration command.

**Examples**

This example shows how to reset the prompt string to its previous setting:

```
switch: unset PS1
switch:
```

**Related Commands**

Command	Description
<a href="#">set</a>	Sets or displays environment variables.

# version

Use the **version** boot loader command to display the boot loader version.

**version**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Modes** Boot loader

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

---

---

**Examples** This example shows how to display the boot loader version:

```
switch: version
switch-name Boot Loader (xxxxx-HBOOT-M) Version 12.2(xx)EX
Compiled Wed 12-Sept-05 14:58 by devgoyal

switch:
```

■ version





## APPENDIX **B**

# Cisco ME 3400E Ethernet Access Switch Debug Commands

---

Please confirm whether or not the This appendix describes the **debug** privileged EXEC commands that have been created or changed for use with the Cisco ME 3400E Ethernet Access switch. These commands are helpful in diagnosing and resolving internetworking problems and should be enabled only under the guidance of Cisco technical support staff.



### Caution

---

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use the **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. It is best to use the **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

---

# debug backup

Use the **debug backup** privileged EXEC command to enable debugging of the Flex Links backup interface. Use the **no** form of this command to disable debugging.

**debug backup** {all | errors | events | vlan-load-balancing}

**no debug backup** {all | errors | events | vlan-load-balancing}

Syntax Description		
	<b>all</b>	Display all backup interface debug messages.
	<b>errors</b>	Display backup interface error or exception debug messages.
	<b>events</b>	Display backup interface event debug messages.
	<b>vlan-load-balancing</b>	Display backup interface VLAN load balancing.

**Command Default** Backup interface debugging is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

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

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug dot1x

Use the **debug dot1x** privileged EXEC command to enable debugging of the IEEE 802.1x feature. Use the **no** form of this command to disable debugging.

```
debug dot1x {all | errors | events | packets | registry | state-machine}
```

```
no debug dot1x {all | errors | events | packets | registry | state-machine}
```

## Syntax Description

<b>all</b>	Display all IEEE 802.1x debug messages.
<b>errors</b>	Display IEEE 802.1x error debug messages.
<b>events</b>	Display IEEE 802.1x event debug messages.
<b>packets</b>	Display IEEE 802.1x packet debug messages.
<b>registry</b>	Display IEEE 802.1x registry invocation debug messages.
<b>state-machine</b>	Display state-machine related-events debug messages.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The **undebug dot1x** command is the same as the **no debug dot1x** command.

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.
<a href="#">show dot1x</a>	Displays IEEE 802.1x statistics, administrative status, and operational status for the switch or for the specified port.

# debug etherchannel

Use the **debug etherchannel** privileged EXEC command to enable debugging of the EtherChannel/PAGP shim. This shim is the software module that is the interface between the Port Aggregation Protocol (PAgP) software module and the port manager software module. Use the **no** form of this command to disable debugging.

**debug etherchannel** [**all** | **detail** | **error** | **event** | **idb**]

**no debug etherchannel** [**all** | **detail** | **error** | **event** | **idb**]



## Note

PAGP is available only on network node interfaces (NNIs) or enhanced network interfaces (ENIs).

## Syntax Description

<b>all</b>	(Optional) Display all EtherChannel debug messages.
<b>detail</b>	(Optional) Display detailed EtherChannel debug messages.
<b>error</b>	(Optional) Display EtherChannel error debug messages.
<b>event</b>	(Optional) Debug major EtherChannel event messages.
<b>idb</b>	(Optional) Display PAgP interface descriptor block debug messages.



## Note

Though visible in the command-line help strings, the **linecard** keyword is not supported.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

If you do not specify a keyword, all debug messages appear.

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

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.
<b>show etherchannel</b>	Displays EtherChannel information for the channel.

## debug ethernet service

Use the **debug ethernet service** privileged EXEC command to enable debugging of Ethernet customer service instances. Use the **no** form of this command to disable debugging.

```
debug ethernet service { all | api | error | evc [id evc-id] | instance [id id interface-id | interface interface-id] | interface [interface-id] | oam-mgr }
```

```
no debug ethernet service { all | api | error | evc [id evc-id] | instance [id id interface-id | interface interface-id] | interface [interface-id] | oam-mgr }
```

Syntax Description		
<b>all</b>		Display all Ethernet customer-service debug messages.
<b>api</b>		Display debug messages about the interaction between the Ethernet infrastructure and its clients.
<b>error</b>		Display Ethernet customer-service error messages occurring in the Ethernet infrastructure subsystem.
<b>evc</b>		Display Ethernet virtual connection (EVC) debug messages
<b>id</b> <i>evc-id</i>		(Optional) Display EVC debug messages relevant to a specific EVC identifier. The EVC identifier can be a string of from 1 to 100 characters.
<b>instance</b>		Display debug messages related to Ethernet customer-service instances.
<b>id</b> <i>id interface-id</i>		(Optional) Display Ethernet service-instance debug messages for a specific Ethernet service instance ID and interface. The service identifier range is 1 to 4294967295. The interface is a physical interface.
<b>interface</b> <i>interface-id</i>		(Optional) When entered after the <b>instance</b> keyword, display service-instance debug messages for the interface. You must enter an interface ID.
<b>interface</b> [ <i>interface-id</i> ]		Display debugging for Ethernet services on all interfaces or the specified interface.
<b>oam-mgr</b>		Display debug messages for the Ethernet operation, administration, and maintenance (OAM) manager component of the infrastructure.

**Command Default** Ethernet service debugging is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** The **undebg ethernet service** command is the same as the **no debug ethernet service** command.

**■** debug ethernet service

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug interface

Use the **debug interface** privileged EXEC command to enable debugging of interface-related activities. Use the **no** form of this command to disable debugging.

```
debug interface {interface-id | null interface-number | port-channel port-channel-number |
vlan vlan-id}
```

```
no debug interface {interface-id | null interface-number | port-channel port-channel-number |
vlan vlan-id}
```

Syntax Description		
<i>interface-id</i>		Display debug messages for the specified physical port, identified by type switch number/module number/ port, for example <b>gigabitethernet 0/2</b> .
<b>null</b> <i>interface-number</i>		Display debug messages for null interfaces. The <i>interface-number</i> is always <b>0</b> .
<b>port-channel</b> <i>port-channel-number</i>		Display debug messages for the specified EtherChannel port-channel interface. The <i>port-channel-number</i> range is 1 to 48.
<b>vlan</b> <i>vlan-id</i>		Display debug messages for the specified VLAN. The <i>vlan-id</i> range is 1 to 4094.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** If you do not specify a keyword, all debug messages appear. The **undebg interface** command is the same as the **no debug interface** command.

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.
	<b>show etherchannel</b>	Displays EtherChannel information for the channel.

# debug ip dhcp snooping

Use the **debug ip dhcp snooping** privileged EXEC command to enable debugging of DHCP snooping. Use the **no** form of this command to disable debugging.

**debug ip dhcp snooping** {*mac-address* | **agent** | **event** | **packet**}

**no debug ip dhcp snooping** {*mac-address* | **agent** | **event** | **packet**}

## Syntax Description

<i>mac-address</i>	Display debug messages for a DHCP packet with the specified MAC address.
<b>agent</b>	Display debug messages for DHCP snooping agents.
<b>event</b>	Display debug messages for DHCP snooping events.
<b>packet</b>	Display debug messages for DHCP snooping.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The **undebug ip dhcp snooping** command is the same as the **no debug ip dhcp snooping** command.

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.



# debug ip igmp filter

Use the **debug ip igmp filter** privileged EXEC command to enable debugging of Internet Group Management Protocol (IGMP) filter events. Use the **no** form of this command to disable debugging.

**debug ip igmp filter**

**no debug ip igmp filter**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** The **undebug ip igmp filter** command is the same as the **no debug ip igmp filter** command.

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.

## debug ip igmp max-groups

Use the **debug ip igmp max-groups** privileged EXEC command to enable debugging of Internet Group Management Protocol (IGMP) maximum groups events. Use the **no** form of this command to disable debugging.

**debug ip igmp max-groups**

**no debug ip igmp max-groups**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** Debugging is disabled.

---

**Command Modes** Privileged EXEC

---

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

---



---

**Usage Guidelines** The **undebug ip igmp max-groups** command is the same as the **no debug ip igmp max-groups** command.

---

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.

---

# debug ip igmp snooping

Use the **debug igmp snooping** privileged EXEC command to enable debugging of Internet Group Management Protocol (IGMP) snooping activity. Use the **no** form of this command to disable debugging.

**debug ip igmp snooping** [**group** | **management** | **querier** | **router** | **timer**]

**no debug ip igmp snooping** [**group** | **management** | **querier** | **router** | **timer**]

Syntax Description	
<b>group</b>	(Optional) Display IGMP snooping group activity debug messages.
<b>management</b>	(Optional) Display IGMP snooping management activity debug messages.
<b>querier</b>	(Optional) Display IGMP snooping querier debug messages.
<b>router</b>	(Optional) Display IGMP snooping router activity debug messages.
<b>timer</b>	(Optional) Display IGMP snooping timer event debug messages.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** The **undebug ip igmp snooping** command is the same as the **no debug ip igmp snooping** command.

Related Commands	Command	Description
	<a href="#">debug platform ip igmp snooping</a>	Displays information about platform-dependent IGMP snooping activity.
	<a href="#">show debugging</a>	Displays information about the types of debugging that are enabled.

## debug ip sla error twamp connection

Use the **debug ip sla error twamp connection** command in privileged EXEC mode to enable debugging output of Cisco IOS IP Service Level Agreements (SLAs) Two-Way Active Measurement Protocol (TWAMP) showing exceptions during communication between the TWAMP client and server. Use the **no** form of this command to disable debugging output.

**debug ip sla error twamp connection** [**source-ip** *ip-address*]

**no debug ip sla error twamp connection** [**source-ip** *ip-address*]

### Syntax Description

<b>source-ip</b> <i>ip-address</i>	(Optional) Debug IP Performance Metrics (IPPM) TWAMP connections for the specified source. Specify the source using the IP address of the client device.
---------------------------------------	--

### Command Modes

Privileged EXEC

### Command History

Release	Modification
12.2(52)SE	This command was introduced.

### Usage Guidelines

The **debug ip sla error twamp connection** privileged EXEC command displays messages about the exceptions that occurred during TWAMP communications between the server and reflector.

The **undebug ip sla error twamp connection** command is the same as the **no debug ip sla error twamp connection** command.



#### Note

Use the **debug ip sla error twamp connection** command before using the **debug ip sla trace twamp connection** command because the **debug ip sla error twamp connection** command generates less debugging output.

The **debug ip sla error twamp connection** command is supported in IPv4 networks.

### Related Commands

Command	Description
<a href="#">debug ip sla error twamp control reflector</a>	Displays exceptions during communication between the IP SLAs TWAMP server and reflector.
<a href="#">debug ip sla error twamp control server</a>	Displays exceptions during communication between the IP SLAs TWAMP server and reflector.
<a href="#">debug ip sla error twamp session</a>	Displays exceptions during communication between the IP SLAs TWAMP sender and reflector.
<a href="#">debug ip sla trace twamp connection</a>	Displays the normal communications between an IP SLAs TWAMP client and server.

<b>debug ip sla trace twamp control reflector</b>	Displays the normal communications sent by an IP SLAs TWAMP reflector to the TWAMP server.
<b>debug ip sla trace twamp control server</b>	Displays the normal communications sent by an IP SLAs TWAMP server to the TWAMP reflector.
<b>debug ip sla trace twamp session</b>	Displays the normal communications between an IP SLAs TWAMP sender and reflector.
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug ip sla error twamp control reflector

Use the **debug ip sla error twamp control reflector** command in privileged EXEC mode to enable debugging output of Cisco IOS IP Service Level Agreements (SLAs) Two-Way Active Measurement Protocol (TWAMP) showing exceptions during communication between the TWAMP server and reflector. Use the **no** form of this command to disable debugging output.

**debug ip sla error twamp control reflector**

**no debug ip sla error twamp control reflector**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(52)SE	This command was introduced.

**Usage Guidelines** The **debug ip sla error twamp control reflector** privileged EXEC command displays messages about exceptions that occurred during communications sent from the TWAMP session reflector to the TWAMP session server.



**Note**

Use the **debug ip sla error twamp control reflector** command before using the **debug ip sla trace twamp control reflector** command because the **debug ip sla error twamp control reflector** command generates less debugging output.

The **debug ip sla error twamp control reflector** command is supported in IPv4 networks.

The **undebug ip sla error twamp control reflector** command is the same as the **no debug ip sla error twamp control reflector** command.

Related Commands	Command	Description
	<a href="#">debug ip sla error twamp connection</a>	Displays exceptions during communication between the IP SLAs TWAMP client and server.
	<a href="#">debug ip sla error twamp control server</a>	Displays exceptions during communication between the IP SLAs TWAMP server and reflector.
	<a href="#">debug ip sla error twamp session</a>	Displays exceptions during communication between the IP SLAs TWAMP sender and reflector.
	<a href="#">debug ip sla trace twamp connection</a>	Displays the normal communications between an IP SLAs TWAMP client and server.
	<a href="#">debug ip sla error twamp control reflector</a>	Displays the normal communications sent by an IP SLAs TWAMP reflector to the TWAMP server.

<b>debug ip sla trace twamp control server</b>	Displays the normal communications sent by an IP SLAs TWAMP server to the TWAMP reflector.
<b>debug ip sla trace twamp session</b>	Displays the normal communications between an IP SLAs TWAMP sender and reflector.
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug ip sla error twamp control server

Use the **debug ip sla error twamp control server** command in privileged EXEC mode to enable debugging output of Cisco IOS IP Service Level Agreements (SLAs) Two-Way Active Measurement Protocol (TWAMP) exceptions during communication between the TWAMP server and reflector. Use the **no** form of this command to disable debugging output.

**debug ip sla error twamp control server**

**no debug ip sla error twamp control server**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(52)SE	This command was introduced.

**Usage Guidelines** The **debug ip sla error twamp control server** privileged EXEC command displays messages about exceptions that occurred during communications sent from the TWAMP session server to the TWAMP session reflector.



**Note**

Use the **debug ip sla error twamp control server** command before using the **debug ip sla trace twamp control server** command because the **debug ip sla error twamp control server** command generates less debugging output.

The **debug ip sla error twamp control server** command is supported in IPv4 networks.

The **undebug ip sla error twamp control server** command is the same as the **no debug ip sla error twamp control server** command.

Related Commands	Command	Description
	<a href="#">debug ip sla error twamp connection</a>	Displays exceptions during communication between the IP SLAs TWAMP client and server.
	<a href="#">debug ip sla error twamp control reflector</a>	Displays exceptions during communication between the IP SLAs TWAMP server and reflector.
	<a href="#">debug ip sla error twamp session</a>	Displays exceptions during communication between the IP SLAs TWAMP sender and reflector.
	<a href="#">debug ip sla error twamp connection</a>	Displays the normal communications between an IP SLAs TWAMP client and server.
	<a href="#">debug ip sla trace twamp control reflector</a>	Displays the normal communications sent by an IP SLAs TWAMP reflector to the TWAMP server.



<b>debug ip sla trace twamp control server</b>	Displays the normal communications sent by an IP SLAs TWAMP server to the TWAMP reflector.
<b>debug ip sla trace twamp session</b>	Displays the normal communications between an IP SLAs TWAMP sender and reflector.
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug ip sla error twamp session

Use the **debug ip sla error twamp session** command in privileged EXEC mode to enable debugging output of Cisco IOS IP Service Level Agreements (SLAs) Two-Way Active Measurement Protocol (TWAMP) showing exceptions during communication between the TWAMP sender and reflector. Use the **no** form of this command to disable debugging output.

**debug ip sla error twamp session** [**source-ip** *ip-address*]

**no debug ip sla error twamp session** [**source-ip** *ip-address*]

## Syntax Description

<b>source-ip</b> <i>ip-address</i>	(Optional) Debug IP Performance Metrics (IPPM) TWAMP connections for the specified source. Specify the source using the IP address of the client device.
---------------------------------------	--

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(52)SE	This command was introduced.

## Usage Guidelines

The **debug ip sla error twamp session** privileged EXEC command displays error messages about the communication between the TWAMP sender and reflector.



### Note

Use the **debug ip sla error twamp session** command before using the **debug ip sla trace twamp session** command because the **debug ip sla error twamp session** command generates less debugging output.

The **debug ip sla error twamp session** command is supported in IPv4 networks.

The **undebug ip sla error twamp session** command is the same as the **no debug ip sla error twamp session** command.

## Related Commands

Command	Description
<a href="#">debug ip sla error twamp connection</a>	Displays exceptions during communication between the IP SLAs TWAMP client and server.
<a href="#">debug ip sla error twamp control reflector</a>	Displays exceptions during communication between the IP SLAs TWAMP server and reflector.
<a href="#">debug ip sla error twamp control server</a>	Displays exceptions during communication between the IP SLAs TWAMP server and reflector.
<a href="#">debug ip sla trace twamp connection</a>	Displays the normal communications between an IP SLAs TWAMP client and server.
<a href="#">debug ip sla trace twamp control reflector</a>	Displays the normal communications sent by an IP SLAs TWAMP reflector to the TWAMP server.

<b>debug ip sla trace twamp control server</b>	Displays the normal communications sent by an IP SLAs TWAMP server to the TWAMP reflector.
<b>debug ip sla trace twamp session</b>	Displays the normal communications between an IP SLAs TWAMP sender and reflector.
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug ip sla trace twamp connection

Use the **debug ip sla trace twamp connection** command in privileged EXEC mode to display the normal communications between a Cisco IOS IP Service Level Agreements (SLAs) Two-Way Active Measurement Protocol (TWAMP) client and server. Use the **no** form of this command to disable debugging output.

```
debug ip sla trace twamp connection [source-ip ip-address]
```

```
no debug ip sla trace twamp connection [source-ip ip-address]
```

## Syntax Description

<b>source-ip ip-address</b>	(Optional) Debug IP Performance Metrics (IPPM) TWAMP connections for the specified source. Specify the source using the client device IP address.
-----------------------------	---

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(52)SE	This command was introduced.

## Usage Guidelines

The **debug ip sla trace twamp connection** privileged EXEC command displays messages about normal communications between the client and server during a TWAMP session.



### Note

Use the **debug ip sla error twamp connection** command before using the **debug ip sla trace twamp connection** command because the **debug ip sla error twamp connection** command generates less debugging output.

The **debug ip sla trace twamp connection** command is supported in IPv4 networks.

The **undebug ip sla trace twamp connection** command is the same as the **no debug ip sla trace twamp connection** command.

## Related Commands

Command	Description
<a href="#">debug ip sla error twamp connection</a>	Displays exceptions during communication between the IP SLAs TWAMP client and server.
<a href="#">debug ip sla error twamp control reflector</a>	Displays exceptions during communication between the IP SLAs TWAMP server and reflector.
<a href="#">debug ip sla error twamp control server</a>	Displays exceptions during communication between the IP SLAs TWAMP server and reflector.
<a href="#">debug ip sla error twamp session</a>	Displays exceptions during communication between the IP SLAs TWAMP sender and reflector.
<a href="#">debug ip sla trace twamp control reflector</a>	Displays the normal communications sent by an IP SLAs TWAMP reflector to the TWAMP server.

<b>debug ip sla error twamp control server</b>	Displays the normal communications sent by an IP SLAs TWAMP server to the TWAMP reflector.
<b>debug ip sla trace twamp session</b>	Displays the normal communications between an IP SLAs TWAMP sender and reflector.
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug ip sla trace twamp control reflector

Use the **debug ip sla trace twamp control reflector** command in privileged EXEC mode to enable debugging output of Cisco IOS IP Service Level Agreements (SLAs) Two-Way Active Measurement Protocol (TWAMP) normal communications between the TWAMP server and reflector. Use the **no** form of this command to disable debugging output.

**debug ip sla trace twamp control reflector**

**no debug ip sla trace twamp control reflector**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(52)SE	This command was introduced.

**Usage Guidelines** The **debug ip sla trace twamp control reflector** privileged EXEC command displays messages about normal TWAMP session communications sent from the reflector to the server.



**Note**

Use the **debug ip sla error twamp control reflector** command before using the **debug ip sla trace twamp control reflector** command because the **debug ip sla error twamp control reflector** command generates less debugging output.

The **debug ip sla trace twamp control reflector** command is supported in IPv4 networks.

The **undebug ip sla trace twamp control reflector** command is the same as the **no debug ip sla trace twamp control reflector** command.

Related Commands	Command	Description
	<a href="#">debug ip sla error twamp connection</a>	Displays exceptions during communication between the IP SLAs TWAMP client and server.
	<a href="#">debug ip sla error twamp control reflector</a>	Displays exceptions during communication between the IP SLAs TWAMP server and reflector.
	<a href="#">debug ip sla error twamp control server</a>	Displays exceptions during communication between the IP SLAs TWAMP server and reflector.
	<a href="#">debug ip sla error twamp session</a>	Displays exceptions during communication between the IP SLAs TWAMP sender and reflector.
	<a href="#">debug ip sla trace twamp connection</a>	Displays the normal communications between an IP SLAs TWAMP client and server.

<b>debug ip sla trace twamp control server</b>	Displays the normal communications sent by an IP SLAs TWAMP server to the TWAMP reflector.
<b>debug ip sla trace twamp session</b>	Displays the normal communications between an IP SLAs TWAMP sender and reflector.
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug ip sla trace twamp control server

Use the **debug ip sla trace twamp control server** command in privileged EXEC mode to enable debugging output of Cisco IOS IP Service Level Agreements (SLAs) Two-Way Active Measurement Protocol (TWAMP) normal communications between the TWAMP server and reflector. Use the **no** form of this command to disable debugging output.

**debug ip sla trace twamp control server**

**no debug ip sla trace twamp control server**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(52)SE	This command was introduced.

**Usage Guidelines** The **debug ip sla trace twamp control server** privileged EXEC command displays messages about normal TWAMP session communications sent from the server to the reflector.



**Note**

Use the **debug ip sla error twamp control server** command before using the **debug ip sla trace twamp control server** command because the **debug ip sla error twamp control server** command generates less debugging output.

The **debug ip sla trace twamp control server** command is supported in IPv4 networks.

The **undebug ip sla trace twamp control server** command is the same as the **no debug ip sla trace twamp control server** command.

Related Commands	Command	Description
	<a href="#">debug ip sla error twamp connection</a>	Displays exceptions during communication between the IP SLAs TWAMP client and server.
	<a href="#">debug ip sla error twamp control reflector</a>	Displays exceptions during communication between the IP SLAs TWAMP server and reflector.
	<a href="#">debug ip sla error twamp control server</a>	Displays exceptions during communication between the IP SLAs TWAMP server and reflector.
	<a href="#">debug ip sla error twamp session</a>	Displays exceptions during communication between the IP SLAs TWAMP sender and reflector.
	<a href="#">debug ip sla trace twamp connection</a>	Displays the normal communications between an IP SLAs TWAMP client and server.



<b>debug ip sla trace twamp control reflector</b>	Displays the normal communications sent by an IP SLAs TWAMP reflector to the TWAMP server.
<b>debug ip sla trace twamp session</b>	Displays the normal communications between an IP SLAs TWAMP sender and reflector.
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug ip sla trace twamp session

Use the **debug ip sla trace twamp session** command in privileged EXEC mode to enable debugging output of Cisco IOS IP Service Level Agreements (SLAs) Two-Way Active Measurement Protocol (TWAMP) normal session communication between the TWAMP sender and reflector. Use the **no** form of this command to disable debugging output.

**debug ip sla trace twamp session** [**source-ip** *ip-address* | **source-port** *port-number*]

**no debug ip sla trace twamp session** [**source-ip** *ip-address* | **source-port** *port-number*]

## Syntax Description

<b>source-ip</b> <i>ip-address</i>	(Optional) Debug IP Performance Metrics (IPPM) TWAMP connections for the specified source. Specify the source using the client device IP address.
<b>source-port</b> <i>port-number</i>	(Optional) Debug IP Performance Metrics (IPPM) TWAMP connections for the specified port.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(52)SE	This command was introduced.

## Usage Guidelines

The **debug ip sla trace twamp session** privileged EXEC command displays normal session communication between the TWAMP sender and reflector.



### Note

Use the **debug ip sla error twamp session** command before using the **debug ip sla trace twamp session** command because the **debug ip sla error twamp session** command generates less debugging output.

The **debug ip sla trace twamp session** command is supported in IPv4 networks.

The **undebug ip sla trace twamp session** command is the same as the **no debug ip sla trace twamp session** command.

## Related Commands

Command	Description
<a href="#">debug ip sla error twamp connection</a>	Displays exceptions during communication between the IP SLAs TWAMP client and server.
<a href="#">debug ip sla error twamp control reflector</a>	Displays exceptions during communication between the IP SLAs TWAMP server and reflector.
<a href="#">debug ip sla error twamp control server</a>	Displays exceptions during communication between the IP SLAs TWAMP server and reflector.
<a href="#">debug ip sla error twamp session</a>	Displays exceptions during communication between the IP SLAs TWAMP sender and reflector.

<b>debug ip sla trace twamp connection</b>	Displays the normal communications between an IP SLAs TWAMP client and server.
<b>debug ip sla trace twamp control reflector</b>	Displays the normal communications sent by an IP SLAs TWAMP reflector to the TWAMP server.
<b>debug ip sla trace twamp control server</b>	Displays the normal communications sent by an IP SLAs TWAMP server to the TWAMP reflector.
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug ip verify source packet

Use the **debug ip verify source packet** privileged EXEC command to enable debugging of IP source guard. Use the **no** form of this command to disable debugging.

**debug ip verify source packet**

**no debug ip verify source packet**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** The **undebug ip verify source packet** command is the same as the **no debug ip verify source packet** command.

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug lacp

Use the **debug lacp** privileged EXEC command to enable debugging of Link Aggregation Control Protocol (LACP) activity. Use the **no** form of this command to disable debugging.

**debug lacp** [**all** | **event** | **fsm** | **misc** | **packet**]

**no debug lacp** [**all** | **event** | **fsm** | **misc** | **packet**]



## Note

LACP is available only on network node interfaces (NNIs) and enhanced network interfaces (ENIs).

## Syntax Description

<b>all</b>	(Optional) Display all LACP debug messages.
<b>event</b>	(Optional) Display LACP event debug messages.
<b>fsm</b>	(Optional) Display LACP finite state-machine debug messages.
<b>misc</b>	(Optional) Display miscellaneous LACP debug messages.
<b>packet</b>	(Optional) Display LACP packet debug messages.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

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

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.
<b>show lacp</b>	Displays LACP channel-group information.

# debug mac-notification

Use the **debug mac-notification** privileged EXEC command to enable debugging of MAC notification events. Use the **no** form of this command to disable debugging.

**debug mac-notification**

**no debug mac-notification**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** Debugging is disabled.

---

**Command Modes** Privileged EXEC

---

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

---



---

**Usage Guidelines** The **undebug mac-notification** command is the same as the **no debug mac-notification** command.

---

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.
	<a href="#">show mac address-table notification</a>	Displays the MAC address notification information for all interfaces or the specified interface.

---

# debug matm

Use the **debug matm** privileged EXEC command to enable debugging of platform-independent MAC address management. Use the **no** form of this command to disable debugging.

**debug matm**

**no debug matm**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

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

Related Commands	Command	Description
	<a href="#">debug platform matm</a>	Displays information about platform-dependent MAC address management.
	<a href="#">show debugging</a>	Displays information about the types of debugging that are enabled.

# debug matm move update

Use the **debug matm move update** privileged EXEC command to enable debugging of MAC address-table move update message processing.

**debug matm move update**

**no debug matm move update**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** Debugging is disabled.

---

**Command Modes** Privileged EXEC

---

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

---



---

**Usage Guidelines** The **undebg matm move update** command is the same as the **no debug matm move update** command.

---

Related Commands	Command	Description
	<a href="#">mac address-table move update</a>	Configures the MAC address-table move update feature on the switch.
	<a href="#">show debugging</a>	Displays information about the types of debugging that are enabled.
	<a href="#">show mac address-table move update</a>	Displays the MAC address-table move update information on the switch.

---



# debug monitor

Use the **debug monitor** privileged EXEC command to enable debugging of the Switched Port Analyzer (SPAN) feature. Use the **no** form of this command to disable debugging.

**debug monitor** { **all** | **errors** | **idb-update** | **info** | **list** | **notifications** | **platform** | **requests** | **snmp** }

**no debug monitor** { **all** | **errors** | **idb-update** | **info** | **list** | **notifications** | **platform** | **requests** | **snmp** }

Syntax	Description
<b>all</b>	Display all SPAN debug messages.
<b>errors</b>	Display detailed SPAN error debug messages.
<b>idb-update</b>	Display SPAN interface description block (IDB) update-trace debug messages.
<b>info</b>	Display SPAN informational-tracing debug messages.
<b>list</b>	Display SPAN port and VLAN-list tracing debug messages.
<b>notifications</b>	Display SPAN notification debug messages.
<b>platform</b>	Display SPAN platform-tracing debug messages.
<b>requests</b>	Display SPAN request debug messages.
<b>snmp</b>	Display SPAN and Simple Network Management Protocol (SNMP) tracing debug messages.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

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

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.
	<b>show monitor</b>	Displays information about all SPAN and remote SPAN (RSPAN) sessions on the switch.

# debug mvrdbg

Use the **debug mvrdbg** privileged EXEC command to enable debugging of Multicast VLAN Registration (MVR). Use the **no** form of this command to disable debugging.

```
debug mvrdbg {all | events | igmpsn | management | ports}
```

```
no debug mvrdbg {all | events | igmpsn | management | ports}
```

## Syntax Description

<b>all</b>	Display all MVR activity debug messages.
<b>events</b>	Display MVR event-handling debug messages.
<b>igmpsn</b>	Display MVR Internet Group Management Protocol (IGMP) snooping-activity debug messages.
<b>management</b>	Display MVR management-activity debug messages.
<b>ports</b>	Display MVR port debug messages.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

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

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.
<b>show mvr</b>	Displays the current MVR configuration.

# debug nvram

Use the **debug nvram** privileged EXEC command to enable debugging of NVRAM activity. Use the **no** form of this command to disable debugging.

**debug nvram**

**no debug nvram**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

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

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug pagp

Use the **debug pagp** privileged EXEC command to enable debugging of Port Aggregation Protocol (PAgP) activity. Use the **no** form of this command to disable debugging.

**debug pagp** [**all** | **event** | **fsm** | **misc** | **packet**]

**no debug pagp** [**all** | **event** | **fsm** | **misc** | **packet**]



## Note

PAgP is available only on network node interfaces (NNIs) and enhanced network interfaces (ENIs).

## Syntax Description

<b>all</b>	(Optional) Display all PAgP debug messages.
<b>event</b>	(Optional) Display PAgP event debug messages.
<b>fsm</b>	(Optional) Display PAgP finite state-machine debug messages.
<b>misc</b>	(Optional) Display miscellaneous PAgP debug messages.
<b>packet</b>	(Optional) Display PAgP packet debug messages.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

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

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.
<b>show pagp</b>	Displays PAgP channel-group information.

# debug platform acl

Use the **debug platform acl** privileged EXEC command to enable debugging of the access control list (ACL) manager. Use the **no** form of this command to disable debugging.

```
debug platform acl {all | exit | label | main | vacl | vmap | warn}
```

```
no debug platform acl {all | exit | label | main | vacl | vmap | warn}
```

## Syntax Description

<b>all</b>	Display all ACL manager debug messages.
<b>exit</b>	Display ACL exit-related debug messages.
<b>label</b>	Display ACL label-related debug messages.
<b>main</b>	Display the main or important ACL debug messages.
<b>racl</b>	Display router ACL related debug messages.
<b>vacl</b>	Display VLAN ACL-related debug messages.
<b>vmap</b>	Display ACL VLAN-map-related debug messages.
<b>warn</b>	Display ACL warning-related debug messages.



## Note

Though visible in the command-line help strings, the **stack** keyword is not supported.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The **undebug platform acl** command is the same as the **no debug platform acl** command.

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug platform backup interface

Use the **debug platform backup interface** privileged EXEC command to enable debugging of the Flex Links platform backup interface. Use the **no** form of this command to disable debugging.

**debug platform backup interface**

**no debug platform backup interface**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Platform backup interface debugging is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

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

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug platform cfm

Use the **debug platform cfm** privileged EXEC command to enable debugging of the Ethernet Connectivity Fault Management (CFM) service. Use the **no** form of this command to disable debugging.

**debug platform cfm**

**no debug platform cfm**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** CFM is an end-to-end, per-service-instance, Ethernet layer operation, administration, and management (OAM) protocol. It provides connectivity monitoring, fault verification, and fault isolation for large Ethernet networks.

The **undebg platform cfm** command is the same as the **no debug platform cfm** command.

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug platform cpu-queues

Use the **debug platform cpu-queues** privileged EXEC command to enable debugging of platform central processing unit (CPU) receive queues. Use the **no** form of this command to disable debugging.

```
debug platform cpu-queues {broadcast-q | cbt-to-spt-q | cpuhub-q | host-q | icmp-q |
  igmp-snooping-q | layer2-protocol-q | logging-q | remote-console-q | routing-protocol-q |
  rpffail-q | software-fwd-q | stp-q}
```

```
no debug platform cpu-queues {broadcast-q | cbt-to-spt-q | cpuhub-q | host-q | icmp-q |
  igmp-snooping-q | layer2-protocol-q | logging-q | remote-console-q | routing-protocol-q |
  rpffail-q | software-fwd-q | stp-q}
```

Syntax Description		
<b>broadcast-q</b>	Display debug messages about packets received by the broadcast queue.	
<b>cbt-to-spt-q</b>	Display debug messages about packets received by the core-based tree to shortest-path tree (cbt-to-spt) queue.	
<b>cpuhub-q</b>	Display debug messages about packets received by the CPU heartbeat queue.	
<b>host-q</b>	Display debug messages about packets received by the host queue.	
<b>icmp-q</b>	Display debug messages about packets received by the Internet Control Message Protocol (ICMP) queue.	
<b>igmp-snooping-q</b>	Display debug messages about packets received by the Internet Group Management Protocol (IGMP)-snooping queue.	
<b>layer2-protocol-q</b>	Display debug messages about packets received by the Layer 2 protocol queue.	
<b>logging-q</b>	Display debug messages about packets received by the logging queue.	
<b>remote-console-q</b>	Display debug messages about packets received by the remote console queue.	
<b>routing-protocol-q</b>	Display debug messages about packets received by the routing protocol queue.	
<b>rpffail-q</b>	Display debug messages about packets received by the reverse path forwarding (RFP) failure queue.	
<b>software-fwd-q</b>	Debug packets received by the software forwarding queue.	
<b>stp-q</b>	Debug packets received by the Spanning Tree Protocol (STP) queue.	

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** The **undebug platform cpu-queues** command is the same as the **no debug platform cpu-queues** command.



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

# debug platform dot1ad

To enable debugging of IEEE 802.1ad tagging, use the **debug platform dot1ad** privileged EXEC command. To disable debugging, use the **no** form of the command.

**debug platform dot1ad** [error | events | receive | transmit]

**no debug platform dot1ad** [error | events | receive | transmit]

## Syntax Description

<b>error</b>	Displays 802.1ad error messages.
<b>events</b>	Displays 802.1ad event debug messages.
<b>receive</b>	Displays 802.1ad receive debug messages.
<b>transmit</b>	Displays 802.1ad sent debug messages.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(54)SE	This command was introduced.

## Usage Guidelines

The **undebug platform dot1ad** command is the same as the **no debug platform dot1ad** command. When you enter **debug platform dot1ad** with no keywords, all 802.1ad debug messages appear.

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the enabled types of debugging.

# debug platform dot1x

Use the **debug platform dot1x** privileged EXEC command to enable debugging of IEEE 802.1x events. Use the **no** form of this command to disable debugging.

```
debug platform dot1x {initialization | interface-configuration | rpc}
```

```
no debug platform dot1x {initialization | interface-configuration | rpc}
```

## Syntax Description

<b>initialization</b>	Display IEEE 802.1x initialization sequence debug messages.
<b>interface-configuration</b>	Display IEEE 802.1x interface configuration-related debug messages.
<b>rpc</b>	Display IEEE 802.1x remote procedure call (RPC) request debug messages.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The **undebug platform dot1x** command is the same as the **no debug platform dot1x** command.

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug platform etherchannel

Use the **debug platform etherchannel** privileged EXEC command to enable debugging of platform-dependent EtherChannel events. Use the **no** form of this command to disable debugging.

**debug platform etherchannel {init | link-up | rpc-detailed | rpc-generic | warnings}**

**no debug platform etherchannel {init | link-up | rpc-detailed | rpc-generic | warnings}**

## Syntax Description

<b>init</b>	Display EtherChannel module initialization debug messages.
<b>link-up</b>	Display EtherChannel link-up and link-down related debug messages.
<b>rpc-detailed</b>	Display detailed EtherChannel remote procedure call (RPC) debug messages.
<b>rpc-generic</b>	Display EtherChannel RPC generic debug messages.
<b>warnings</b>	Display EtherChannel warning debug messages.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

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

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug platform forw-tcam

Use the **debug platform forw-tcam** privileged EXEC command to enable debugging of the forwarding ternary content addressable memory (TCAM) manager. Use the **no** form of this command to disable debugging.

**debug platform forw-tcam** [**adjustment** | **allocate** | **audit** | **error** | **move** | **read** | **write**]

**no debug platform forw-tcam** [**adjustment** | **allocate** | **audit** | **error** | **move** | **read** | **write**]

## Syntax Description

<b>adjustment</b>	(Optional) Display TCAM manager adjustment debug messages.
<b>allocate</b>	(Optional) Display TCAM manager allocation debug messages.
<b>audit</b>	(Optional) Display TCAM manager audit messages.
<b>error</b>	(Optional) Display TCAM manager error messages.
<b>move</b>	(Optional) Display TCAM manager move messages.
<b>read</b>	(Optional) Display TCAM manager read messages.
<b>write</b>	(Optional) Display TCAM manager write messages.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

If you do not specify a keyword, all forwarding TCAM manager debug messages appear.

The **undebg platform forw-tcam** command is the same as the **no debug platform forw-tcam** command.

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug platform ip arp inspection

Use the **debug platform ip arp inspection** privileged EXEC command to debug dynamic Address Resolution Protocol (ARP) inspection events. Use the **no** form of this command to disable debugging.

**debug platform ip arp inspection** {all | error | event | packet | rpc}

**no debug platform ip arp inspection** {all | error | event | packet | rpc}

## Syntax Description

<b>all</b>	Display all dynamic ARP inspection debug messages.
<b>error</b>	Display dynamic ARP inspection error debug messages.
<b>event</b>	Display dynamic ARP inspection event debug messages.
<b>packet</b>	Display dynamic ARP inspection packet-related debug messages.
<b>rpc</b>	Display dynamic ARP inspection remote procedure call (RPC) request debug messages.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The **undebug platform ip arp inspection** command is the same as the **no debug platform ip arp inspection** command.

## Related Commands

Command	Description
<a href="#">show ip arp inspection</a>	Displays the dynamic ARP inspection configuration and operating state.
<a href="#">show debugging</a>	Displays information about the types of debugging that are enabled.

# debug platform ip dhcp

Use the **debug platform ip dhcp** privileged EXEC command to debug DHCP events. Use the **no** form of this command to disable debugging.

**debug platform ip dhcp** [**all** | **error** | **event** | **packet** | **rpc**]

**no debug platform ip dhcp** [**all** | **error** | **event** | **packet** | **rpc**]

## Syntax Description

<b>all</b>	(Optional) Display all DHCP debug messages.
<b>error</b>	(Optional) Display DHCP error debug messages.
<b>event</b>	(Optional) Display DHCP event debug messages.
<b>packet</b>	(Optional) Display DHCP packet-related debug messages.
<b>rpc</b>	(Optional) Display DHCP remote procedure call (RPC) request debug messages.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The **undebug platform ip dhcp** command is the same as the **no debug platform ip dhcp** command.

## Related Commands

Command	Description
<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.
<a href="#">show ip dhcp snooping binding</a>	Displays the DHCP snooping binding information.
<a href="#">show debugging</a>	Displays information about the types of debugging that are enabled.

## debug platform ip igmp snooping

Use the **debug platform ip igmp snooping** privileged EXEC command to enable debugging of platform-dependent Internet Group Management Protocol (IGMP) snooping. Use the **no** form of this command to disable debugging.

```
debug platform ip igmp snooping {all | di | error | event | group | mgmt | pak | retry | rpc | warn}
```

```
debug platform ip igmp snooping pak {ip-address | error | ipopt | leave | query | report | rx | svi | tx}
```

```
debug platform ip igmp snooping rpc [cfg | l3mm | misc | vlan]
```

```
no debug platform ip igmp snooping {all | di | error | event | group | mgmt | pak | retry | rpc | warn}
```

Syntax Description		
<b>all</b>		Display all IGMP snooping debug messages.
<b>di</b>		Display IGMP snooping destination index (di) coordination remote procedure call (RPC) debug messages.
<b>error</b>		Display IGMP snooping error messages.
<b>event</b>		Display IGMP snooping event debug messages.
<b>group</b>		Display IGMP snooping group debug messages.
<b>mgmt</b>		Display IGMP snooping management debug messages.
<b>pak</b> { <i>ip-address</i>   <b>error</b>   <b>ipopt</b>   <b>leave</b>   <b>query</b>   <b>report</b>   <b>rx</b>   <b>svi</b>   <b>tx</b> }		Display IGMP snooping packet event debug messages. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <i>ip-address</i>—IP address of the IGMP group.</li> <li>• <b>error</b>—Display IGMP snooping packet error debug messages.</li> <li>• <b>ipopt</b>—Display IGMP snooping IP bridging options debug messages.</li> <li>• <b>leave</b>—Display IGMP snooping leave debug messages.</li> <li>• <b>query</b>—Display IGMP snooping query debug messages.</li> <li>• <b>report</b>—Display IGMP snooping report debug messages.</li> <li>• <b>rx</b>—Display IGMP snooping received packet debug messages.</li> <li>• <b>svi</b>—Display IGMP snooping switched virtual interface (SVI) packet debug messages.</li> <li>• <b>tx</b>—Display IGMP snooping sent packet debug messages.</li> </ul>
<b>private-vlan</b>		Display IGMP snooping private VLAN messages.
<b>retry</b>		Display IGMP snooping retry debug messages.



<b>rpc</b> [ <b>cfg</b>   <b>l3mm</b>   <b>misc</b>   <b>vlan</b> ]	<p>Display IGMP snooping remote procedure call (RPC) event debug messages. The keywords have these meanings:</p> <ul style="list-style-type: none"> <li>• <b>cfg</b>—(Optional) Display IGMP snooping RPC debug messages.</li> <li>• <b>l3mm</b>—(Optional) IGMP snooping Layer 3 multicast router group RPC debug messages.</li> <li>• <b>misc</b>—(Optional) IGMP snooping miscellaneous RPC debug messages.</li> <li>• <b>vlan</b>—(Optional) IGMP snooping VLAN assert RPC debug messages.</li> </ul>
<b>warn</b>	Display IGMP snooping warning messages.

**Defaults**

Debugging is disabled.

**Command Modes**

Privileged EXEC

**Command History**

Release	Modification
12.2(44)EY	This command was introduced.

**Usage Guidelines**

The **undebg platform ip igmp snooping** command is the same as the **no debug platform ip igmp snooping** command.

**Related Commands**

Command	Description
<a href="#">debug ip igmp snooping</a>	Displays information about platform-independent IGMP snooping activity.
<a href="#">show debugging</a>	Displays information about the types of debugging that are enabled.

## debug platform ip multicast

Use the **debug platform ip multicast** privileged EXEC command to enable debugging of IP multicast routing. Use the **no** form of this command to disable debugging.

```
debug platform ip multicast {acl-full-events | all | mdb | mdfs-rp-retry | midb | mroute-rp |
resources | retry | rpf-throttle | snoop-events | software-forward | swidb-events | vlan-locks }
```

```
no debug platform ip multicast {acl-full-events | all | mdb | mdfs-rp-retry | midb | mroute-rp |
resources | retry | rpf-throttle | snoop-events | software-forward | swidb-events | vlan-locks }
```

Syntax Description		
<b>acl-full-events</b>		Display IP-multicast output ACL full debug messages.
<b>all</b>		Display all platform IP-multicast event debug messages.
	<b>Note</b>	Using this command can degrade the performance of the switch.
<b>mdb</b>		Display IP-multicast debug messages for multicast distributed fast switching (MDFS) multicast descriptor block (mdb) events.
<b>mdfs-rp-retry</b>		Display IP-multicast MDFS rendezvous point (RP) retry event debug messages.
<b>midb</b>		Display IP-multicast MDFS multicast interface descriptor block (MIDB) debug messages.
<b>mroute-rp</b>		Display IP-multicast RP event debug messages.
<b>resources</b>		Display IP-multicast hardware resource debug messages.
<b>retry</b>		Display IP-multicast retry processing event debug messages.
<b>rpf-throttle</b>		Display IP-multicast reverse path forwarding (RPF) throttle event debug messages.
<b>snoop-events</b>		Display IP-multicast IGMP snooping event debug messages.
<b>software-forward</b>		Display IP-multicast software forwarding event debug messages.
<b>swidb-events</b>		Display IP-multicast MDFS software interface descriptor block (swidb) or global event debug messages.
<b>vlan-locks</b>		Display IP-multicast VLAN lock and unlock event debug messages.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** The **undebug platform ip multicast** command is the same as the **no debug platform ip multicast** command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug platform ip source-guard

Use the **debug platform ip source-guard** privileged EXEC command to debug IP source guard events. Use the **no** form of this command to disable debugging.

```
debug platform ip source-guard {all | error | event}
```

```
no debug platform ip source-guard {all | error | event}
```

## Syntax Description

<b>all</b>	Display all IP source-guard platform debug messages.
<b>error</b>	Display IP source-guard platform error debug messages.
<b>event</b>	Display IP source-guard platform event debug messages.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(50)SE	This command was introduced.

## Usage Guidelines

The **undebug platform ip source-guard** command is the same as the **no debug platform ip source-guard** command.

## Related Commands

Command	Description
<a href="#">show ip verify source</a>	Displays the IP source guard configuration.
<a href="#">show debugging</a>	Displays information about the types of debugging that are enabled.

# debug platform ip unicast

Use the **debug platform ip unicast** privileged EXEC command to enable debugging of platform-dependent IP unicast routing. Use the **no** form of this command to disable debugging.

```
debug platform ip unicast {adjacency | all | arp | dhcp | errors | events | interface | mpath |
registries | retry | route | rpc | standby | statistics}
```

```
no debug platform ip unicast {adjacency | all | arp | dhcp | errors | events | interface | mpath |
registries | retry | route | rpc | standby | statistics}
```

Syntax Description	
<b>adjacency</b>	Display IP unicast routing adjacency programming event debug messages.
<b>all</b>	Display all platform IP unicast routing debug messages. <b>Note</b> Using this command can degrade the performance of the switch.
<b>arp</b>	Display IP unicast routing Address Resolution Protocol (ARP) and ARP throttling debug messages.
<b>dhcp</b>	Display IP unicast routing DHCP dynamic address-related event debug messages.
<b>errors</b>	Display all IP unicast routing error debug messages, including resource allocation failures.
<b>events</b>	Display all IP unicast routing event debug messages, including registry and miscellaneous events.
<b>interface</b>	Display IP unicast routing interface event debug messages.
<b>mpath</b>	Display IP unicast routing multi-path adjacency programming event debug messages (present when performing equal or unequal cost routing).
<b>registries</b>	Display IP unicast routing forwarding information database (FIB), adjacency add, update, and delete registry event debug messages.
<b>retry</b>	Display IP unicast routing reprogram FIBs with ternary content addressable memory (TCAM) allocation failure debug messages.
<b>route</b>	Display IP unicast routing FIB TCAM programming event debug messages.
<b>rpc</b>	Display IP unicast routing Layer 3 unicast remote procedure call (RPC) interaction debug messages.
<b>standby</b>	Display IP unicast routing standby event debug messages, helpful in troubleshooting Hot Standby Routing Protocol (HSRP) issues.
<b>statistics</b>	Display IP unicast routing statistics gathering-related event debug messages.
<b>table</b>	Display IP unicast routing IPv4 table debug messages.
<b>vrf</b>	Display IP unicast routing VRF debug messages.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

■ **debug platform ip unicast**

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** The **undebbug platform ip unicast** command is the same as the **no debug platform ip unicast** command.

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug platform ipc

Use the **debug platform ipc** privileged EXEC command to enable debugging of the platform-dependent Interprocess Communication (IPC) Protocol. Use the **no** form of this command to disable debugging.

```
debug platform ipc {all | init | receive | send | trace}
```

```
no debug platform {all | init | receive | send | trace}
```

## Syntax Description

<b>all</b>	Display all platform IPC debug messages. <b>Note</b> Using this command can degrade the performance of the switch.
<b>init</b>	Display debug messages related to IPC initialization.
<b>receive</b>	Display IPC traces each time an IPC packet is received by the switch.
<b>send</b>	Display IPC traces each time an IPC packet is sent by the switch.
<b>trace</b>	Display IPC trace debug messages, tracing the code path as the IPC functions are executed.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The **undebug platform ipc** command is the same as the **no debug platform ipc**.

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug platform led

Use the **debug platform led** privileged EXEC command to enable debugging of light-emitting diode (LED) actions. Use the **no** form of this command to disable debugging.

```
debug platform led {generic | signal}
```

```
no debug platform led {generic | signal}
```

## Syntax Description

<b>generic</b>	Display LED generic action debug messages.
<b>signal</b>	Display LED signal bit map debug messages.



## Note

Though visible in the command-line help strings, the **stack** keyword is not supported.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The **undebug platform led** command is the same as the **no debug platform led** command.

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.



# debug platform matm

Use the **debug platform matm** privileged EXEC command to enable debugging of platform-dependent MAC address management. Use the **no** form of this command to disable debugging.

```
debug platform matm {aging | all | ec-aging | errors | learning | rpc | secure-address | warnings}
```

```
no debug platform matm {aging | all | ec-aging | errors | learning | rpc | secure-address | warnings}
```

## Syntax Description

<b>aging</b>	Display MAC address aging debug messages.
<b>all</b>	Display all platform MAC address management event debug messages.
<b>ec-aging</b>	Display EtherChannel address aging-related debug messages.
<b>errors</b>	Display MAC address management error messages.
<b>learning</b>	Display MAC address management address-learning debug messages.
<b>rpc</b>	Display MAC address management remote procedure call (RPC) related debug messages.
<b>secure-address</b>	Display MAC address management secure address learning debug messages.
<b>warning</b>	Display MAC address management warning messages.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The **undebg platform matm** command is the same as the **no debug platform matm** command.

## Related Commands

Command	Description
<a href="#">debug matm</a>	Displays information about platform-independent MAC address management.
<a href="#">show debugging</a>	Displays information about the types of debugging that are enabled.

# debug platform messaging application

Use the **debug platform messaging application** privileged EXEC command to enable debugging of application messaging activity. Use the **no** form of this command to disable debugging.

```
debug platform messaging application {all | badpak | cleanup | events | memerr | messages |
  usererr }
```

```
no debug platform messaging application {all | badpak | cleanup | events | memerr | messages
  | usererr }
```

## Syntax Description

<b>all</b>	Display all application-messaging debug messages.
<b>badpak</b>	Display bad-packet debug messages.
<b>cleanup</b>	Display clean-up debug messages.
<b>events</b>	Display event debug messages.
<b>memerr</b>	Display memory-error debug messages.
<b>messages</b>	Display application-messaging debug messages.
<b>usererr</b>	Display user-error debug messages.



## Note

Though visible in the command-line help strings, the **stackchg** keyword is not supported.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The **undebug platform messaging application** command is the same as the **no debug platform messaging application** command.

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug platform phy

Use the **debug platform phy** privileged EXEC command to enable debugging of PHY driver information. Use the **no** form of this command to disable debugging.

```
debug platform phy { automdix | cablediag | dual-purpose | flcd { configure | ipc | iter | trace } |
  flowcontrol | forced | init-seq | link-status | read | sfp | show-controller | speed | write }
```

```
no debug platform phy { automdix | cablediag | dual-purpose | flcd { configure | ipc | iter | trace }
  | flowcontrol | forced | init-seq | link-status | read | sfp | show-controller | speed | write }
```

## Syntax Description

<b>automdix</b>	Display PHY automatic medium-dependent interface crossover (Auto-MDIX) debug messages.
<b>cablediag</b>	Display PHY cable-diagnostic debug messages.
<b>dual-purpose</b>	Display dual-purpose PHY events.
<b>flcd { configure   ipc   iter   trace }</b>	Display PHY FLCD debug messages. The keywords have these meanings: <ul style="list-style-type: none"> <li><b>configure</b>—Display PHY configure debug messages.</li> <li><b>ipc</b>—Display Interprocess Communication Protocol (IPC) debug messages.</li> <li><b>iter</b>—Display iter debug messages.</li> <li><b>trace</b>—Display trace debug messages.</li> </ul>
<b>flowcontrol</b>	Display PHY flowcontrol debug messages.
<b>forced</b>	Display PHY forced-mode debug messages.
<b>init-seq</b>	Display PHY initialization-sequence debug messages.
<b>link-status</b>	Display PHY link-status debug messages.
<b>read</b>	Display PHY-read debug messages.
<b>sfp</b>	Display PHY small form-factor pluggable (SFP) modules debug messages.
<b>show-controller</b>	Display PHY show-controller debug messages.
<b>speed</b>	Display PHY speed-change debug messages.
<b>write</b>	Display PHY-write debug messages.



### Note

Although visible in the command-line help, the **xenpak** keyword is not supported.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

**■ debug platform phy**

---

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

---

**Related Commands**

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug platform pm

Use the **debug platform pm** privileged EXEC command to enable debugging of the platform-dependent port manager software module. Use the **no** form of this command to disable debugging.

```
debug platform pm {all | counters | errdisable | etherchnl | exceptions | hpm-events | idb-events
| if-numbers | ios-events | link-status | platform | pm-events | pm-vectors [detail] | rpc
[general | oper-info | state | vectors | vp-events] | soutput | 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-vectors [detail]
| rpc [general | oper-info | state | vectors | vp-events] | soutput | sync | vlans }
```

## Syntax Description

<b>all</b>	Display all port-manager debug messages.
<b>counters</b>	Display counters for remote procedure call (RPC) debug messages.
<b>errdisable</b>	Display error-disabled related-events debug messages.
<b>etherchnl</b>	Display EtherChannel related-events debug messages.
<b>exceptions</b>	Display system exception debug messages.
<b>hpm-events</b>	Display platform port-manager event debug messages.
<b>idb-events</b>	Display interface descriptor block (IDB) related-events debug messages.
<b>if-numbers</b>	Display interface-number translation-event debug messages.
<b>ios-events</b>	Display IOS event debug messages.
<b>link-status</b>	Display interface link-detection event debug messages.
<b>platform</b>	Display port-manager function-event debug messages.
<b>pm-events</b>	Display port manager event debug messages.
<b>pm-vectors [detail]</b>	Display port-manager vector-related-event debug messages. The keyword has this meaning: <ul style="list-style-type: none"> <li>• <b>detail</b>—Display vector-function details.</li> </ul>
<b>rpc [general   oper-info   state   vectors   vp-events]</b>	Display RPC related-event debug messages. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>general</b>—(Optional) Display RPC general events.</li> <li>• <b>oper-info</b>—(Optional) Display operational- and informational-related RPC messages.</li> <li>• <b>state</b>—(Optional) Display administrative- and operational-related RPC messages.</li> <li>• <b>vectors</b>—(Optional) Display vector-related RPC messages.</li> <li>• <b>vp-events</b>—(Optional) Display virtual ports related-events RP messages.</li> </ul>
<b>soutput</b>	Display IDB output vector event debug messages.
<b>sync</b>	Display operational synchronization and VLAN line-state event debug messages.
<b>vlans</b>	Display VLAN creation and deletion event debug messages.

**debug platform pm****Note**

Though visible in the command-line help strings, the **stack-manager** keyword is not supported.

**Defaults**

Debugging is disabled.

**Command Modes**

Privileged EXEC

**Command History**

Release	Modification
12.2(44)EY	This command was introduced.

**Usage Guidelines**

The **undebbug platform pm** command is the same as the **no debug platform pm** command.

**Related Commands**

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug platform policer cpu uni-eni

Use the **debug platform policer cpu uni-eni** privileged EXEC command to enable debugging of the control-plane policer for user network interfaces (UNIs) and enhanced network interfaces (ENIs). This command displays information messages when any changes are made to CPU protection. Use the **no** form of this command to disable debugging.

**debug platform policer cpu uni-eni**

**no debug platform policer cpu uni-eni**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** The **undebg platform policer cpu uni-eni** command is the same as the **no debug platform policer cpu uni-eni** command.

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.
	<b>show platform policer cpu</b>	Displays control plane policer statistics per feature or the indexes and the corresponding feature for the specified port.

## debug platform port-asic

Use the **debug platform port-asic** privileged EXEC command to enable debugging of the port application-specific integrated circuit (ASIC) driver. Use the **no** form of this command to disable debugging.

```
debug platform port-asic {interrupt | periodic | read | write}
```

```
no debug platform port-asic {interrupt | periodic | read | write}
```

### Syntax Description

<b>interrupt</b>	Display port-ASIC interrupt-related function debug messages.
<b>periodic</b>	Display port-ASIC periodic-function-call debug messages.
<b>read</b>	Display port-ASIC read debug messages.
<b>write</b>	Display port-ASIC write debug messages.

### Defaults

Debugging is disabled.

### Command Modes

Privileged EXEC

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

The **undebug platform port-asic** command is the same as the **no debug platform port-asic** command.

### Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.



# debug platform port-security

Use the **debug platform port-security** privileged EXEC command to enable debugging of platform-dependent port-security information. Use the **no** form of this command to disable debugging.

**debug platform port-security** {**add** | **aging** | **all** | **delete** | **errors** | **rpc** | **warnings**}

**no debug platform port-security** {**add** | **aging** | **all** | **delete** | **errors** | **rpc** | **warnings**}

## Syntax Description

<b>add</b>	Display secure address addition debug messages.
<b>aging</b>	Display secure address aging debug messages.
<b>all</b>	Display all port-security debug messages.
<b>delete</b>	Display secure address deletion debug messages.
<b>errors</b>	Display port-security error debug messages.
<b>rpc</b>	Display remote procedure call (RPC) debug messages.
<b>warnings</b>	Display warning debug messages.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The **undebg platform port-security** command is the same as the **no debug platform port-security** command.

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

## debug platform qos-acl-tcam

Use the **debug platform qos-acl-tcam** privileged EXEC command to enable debugging of the quality of service (QoS) and access control list (ACL) ternary content addressable memory (TCAM) manager software. Use the **no** form of this command to disable debugging.

```
debug platform qos-acl-tcam {all | ctcam | errors | labels | mask | ms-entry | ms-mask | rpc |
tcam }
```

```
no debug platform qos-acl-tcam {all | ctcam | errors | labels | mask | ms-entry | ms-mask | rpc
| tcam }
```

### Syntax Description

<b>all</b>	Display all QoS and ACL TCAM (QATM) manager debug messages.
<b>ctcam</b>	Display Cisco TCAM (CTCAM) related-events debug messages.
<b>errors</b>	Display QATM error-related-events debug messages.
<b>labels</b>	Display QATM label-related-events debug messages.
<b>mask</b>	Display QATM mask-related-events debug messages.
<b>ms-entry</b>	Display QATM MS-entry-related-events debug messages.
<b>ms-mask</b>	Display QATM MS-mask-related-events debug messages.
<b>rpc</b>	Display QATM remote procedure call (RPC) related-events debug messages.
<b>tcam</b>	Display QATM TCAM-related events debug messages.

### Defaults

Debugging is disabled.

### Command Modes

Privileged EXEC

### Command History

Release	Modification
12.2(44)EY	This command was introduced.

### Usage Guidelines

The **undebug platform qos-acl-tcam** command is the same as the **no debug platform qos-acl-tcam** command.

### Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug platform qos-manager

Use the **debug platform qos-manager** privileged EXEC command to enable debugging of the quality of service (QoS) manager software. Use the **no** form of this command to disable debugging.

**debug platform qos-manager {all | event | verbose}**

**no debug platform qos-manager {all | event | verbose}**

## Syntax Description

<b>all</b>	Display all QoS manager debug messages.
<b>event</b>	Display QoS manager events debug messages.
<b>verbose</b>	Display detailed QoS manager debug messages.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The **undebug platform qos-manager** command is the same as the **no debug platform qos-manager** command.

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug platform remote-commands

Use the **debug platform remote-commands** privileged EXEC command to enable debugging of remote commands. Use the **no** form of this command to disable debugging.

**debug platform remote-commands**

**no debug platform remote-commands**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** Debugging is disabled.

---

**Command Modes** Privileged EXEC

---

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

---



---

**Usage Guidelines** The **undebbug platform remote-commands** command is the same as the **no debug platform remote-commands** command.

---

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.

---

# debug platform rep

Use the **debug platform rep** privileged EXEC command to enable debugging of Resilient Ethernet Protocol (REP). Use the **no** form of this command to disable debugging.

**debug platform rep**

**no debug platform rep**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

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

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug platform resource-manager

Use the **debug platform resource-manager** privileged EXEC command to enable debugging of the resource manager software. Use the **no** form of this command to disable debugging.

**debug platform resource-manager** {all | dm | erd | errors | madmed | sd | stats | vld}

**no debug platform resource-manager** {all | dm | erd | errors | madmed | sd | stats | vld}

## Syntax Description

<b>all</b>	Display all resource manager debug messages.
<b>dm</b>	Display destination-map debug messages.
<b>erd</b>	Display equal-cost-route descriptor-table debug messages.
<b>errors</b>	Display error debug messages.
<b>madmed</b>	Display the MAC address descriptor table and multi-expansion descriptor table debug messages.
<b>sd</b>	Display the station descriptor table debug messages.
<b>stats</b>	Display statistics debug messages.
<b>vld</b>	Display the VLAN-list descriptor debug messages.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The **undebug platform resource-manager** command is the same as the **no debug platform resource-manager** command.

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug platform snmp

Use the **debug platform snmp** privileged EXEC command to enable debugging of the platform-dependent Simple Network Management Protocol (SNMP) software. Use the **no** form of this command to disable debugging.

**debug platform snmp**

**no debug platform snmp**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

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

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug platform span

Use the **debug platform span** privileged EXEC command to enable debugging of the platform-dependent Switched Port Analyzer (SPAN) software. Use the **no** form of this command to disable debugging.

**debug platform span**

**no debug platform span**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** The **undebbug platform span** command is the same as the **no debug platform span** command.

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.



# debug platform supervisor-asic

Use the **debug platform supervisor-asic** privileged EXEC command to enable debugging of the supervisor application-specific integrated circuit (ASIC). Use the **no** form of this command to disable debugging.

```
debug platform supervisor-asic {all | errors | receive | send}
```

```
no debug platform supervisor-asic {all | errors | receive | send}
```

## Syntax Description

<b>all</b>	Display all supervisor-ASIC event debug messages.
<b>errors</b>	Display the supervisor-ASIC error debug messages.
<b>jumbo</b>	Display the supervisor-ASIC jumbo debug messages.
<b>receive</b>	Display the supervisor-ASIC receive debug messages.
<b>send</b>	Display the supervisor-ASIC send debug messages.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The **undebg platform supervisor-asic** command is the same as the **no debug platform supervisor-asic** command.

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug platform sw-bridge

Use the **debug platform sw-bridge** privileged EXEC command to enable debugging of the software bridging function. Use the **no** form of this command to disable debugging.

```
debug platform sw-bridge { broadcast | control | multicast | packet | unicast }
```

```
no debug platform sw-bridge { broadcast | control | multicast | packet | unicast }
```

## Syntax Description

<b>broadcast</b>	Display broadcast-data debug messages.
<b>control</b>	Display protocol-packet debug messages.
<b>multicast</b>	Display multicast-data debug messages.
<b>packet</b>	Display sent and received data debug messages.
<b>unicast</b>	Display unicast-data debug messages.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The **undebug platform sw-bridge** command is the same as the **no debug platform sw-bridge** command.

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

## debug platform tcam

Use the **debug platform tcam** privileged EXEC command to enable debugging of ternary content addressable memory (TCAM) access and lookups. Use the **no** form of this command to disable debugging.

```

debug platform tcam {log | read | search | write}

debug platform tcam log l2 {acl {input | output} | local | qos}

debug platform tcam log l3 {acl {input | output} | local | qos | secondary}

debug platform tcam read {reg | ssram | tcam}

debug platform tcam search

debug platform tcam write {forw-ram | reg | tcam}

no debug platform tcam {log | read | search | write}

no debug platform tcam log l2 {acl {input | output} | local | qos}

no debug platform tcam log l3 {acl {input | output} | local | qos | secondary}

no debug platform tcam read {reg | ssram | tcam}

no debug platform tcam search

no debug platform tcam write {forw-ram | reg | tcam}

```

Syntax	Description
<b>log l2 {acl {input   output}   local   qos}</b>	<p>Display Layer 2 field-based CAM look-up type debug messages. The keywords have these meanings:</p> <ul style="list-style-type: none"> <li>• <b>acl {input   output}</b>—Display input or output ACL look-up debug messages.</li> <li>• <b>local</b>—Display local forwarding look-up debug messages.</li> <li>• <b>qos</b>—Display classification and quality of service (QoS) look-up debug messages.</li> </ul>
<b>l3 {acl {input   output}   local   qos   secondary}</b>	<p>Display Layer 3 field-based CAM look-up type debug messages. The keywords have these meanings:</p> <ul style="list-style-type: none"> <li>• <b>acl {input   output}</b>—Display input or output ACL look-up debug messages.</li> <li>• <b>local</b>—Display local forwarding look-up debug messages.</li> <li>• <b>qos</b>—Display classification and quality of service (QoS) look-up debug messages.</li> <li>• <b>secondary</b>—Display secondary forwarding look-up debug messages.</li> </ul>

<b>read { reg   ssram   tcam }</b>	Display TCAM-read debug messages. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>reg</b>—Display TCAM-register read debug messages.</li> <li>• <b>ssram</b>—Display synchronous static RAM (SSRAM)-read debug messages.</li> <li>• <b>tcam</b>—Display TCAM-read debug messages.</li> </ul>
<b>search</b>	Display supervisor-initiated TCAM-search results debug messages.
<b>write { forw-ram   reg   tcam }</b>	Display TCAM-write debug messages. The keywords have these meanings: <ul style="list-style-type: none"> <li><b>forw-ram</b>—Display forwarding-RAM write debug messages.</li> <li><b>reg</b>—Display TCAM-register write debug messages.</li> <li><b>tcam</b>—Display TCAM-write debug messages.</li> </ul>

**Note**

Though visible in the command-line help strings, the **log l3 ipv6 {acl {input | output} | local | qos | secondary}** keywords are not supported.

**Defaults**

Debugging is disabled.

**Command Modes**

Privileged EXEC

**Command History**

Release	Modification
12.2(44)EY	This command was introduced.

**Usage Guidelines**

The **undebg platform tcam** command is the same as the **no debug platform tcam** command.

**Related Commands**

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug platform udd

Use the **debug platform udd** privileged EXEC command to enable debugging of the platform-dependent UniDirectional Link Detection (UDLD) software. Use the **no** form of this command to disable debugging.

```
debug platform udd [all | error | rpc {events | messages}]
```

```
no debug platform udd [all | error | rpc {events | messages}]
```

## Syntax Description

<b>all</b>	(Optional) Display all UDLD debug messages.
<b>error</b>	(Optional) Display error condition debug messages.
<b>rpc {events   messages}</b>	(Optional) Display UDLD remote procedure call (RPC) debug messages. The keywords have these meanings: <ul style="list-style-type: none"> <li><b>events</b>—Display UDLD RPC events.</li> <li><b>messages</b>—Display UDLD RPC messages.</li> </ul>

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The **undebug platform udd** command is the same as the **no debug platform udd** command.

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug platform vlan

Use the **debug platform vlan** privileged EXEC command to enable debugging of the VLAN manager software. Use the **no** form of this command to disable debugging.

```
debug platform vlan {errors | mvid | rpc}
```

```
no debug platform vlan {errors | mvid | rpc}
```

## Syntax Description

<b>errors</b>	Display VLAN error debug messages.
<b>mvid</b>	Display mapped VLAN ID allocations and free debug messages.
<b>rpc</b>	Display remote procedure call (RPC) debug messages.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The **undebug platform vlan** command is the same as the **no debug platform vlan** command.

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug pm

Use the **debug pm** privileged EXEC command to enable debugging of port manager (PM) activity. The port manager is a state machine that controls all the logical and physical interfaces. All features, such as VLANs, UniDirectional Link Detection (UDLD), and so forth, work with the port manager to provide switch functions. Use the **no** form of this command to disable debugging.

```
debug pm {all | assert | card | cookies | etherchnl | hatable | messages | port | registry | sm | span
          | split | vlan | vp}
```

```
no debug pm {all | assert | card | cookies | etherchnl | hatable | messages | port | registry | sm |
            span | split | vlan | vp}
```

## Syntax Description

<b>all</b>	Display all PM debug messages.
<b>assert</b>	Display assert debug messages.
<b>card</b>	Display line-card related-events debug messages.
<b>cookies</b>	Display internal PM cookie validation debug messages.
<b>etherchnl</b>	Display EtherChannel related-events debug messages.
<b>hatable</b>	Display Host Access Table events debug messages.
<b>messages</b>	Display PM debug messages.
<b>port</b>	Display port related-events debug messages.
<b>registry</b>	Display PM registry invocation debug messages.
<b>sm</b>	Display state-machine related-events debug messages.
<b>span</b>	Display spanning-tree related-events debug messages.
<b>split</b>	Display split-processor debug messages.
<b>vlan</b>	Display VLAN related-events debug messages.
<b>vp</b>	Display virtual port related-events debug messages.



### Note

Though visible in the command-line help strings, the **scp** and **pvlan** keywords are not supported.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

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

■ debug pm

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.



# debug port-security

Use the **debug port-security** privileged EXEC command to enable debugging of the allocation and states of the port security subsystem. Use the **no** form of this command to disable debugging.

**debug port-security**

**no debug port-security**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** The **undebg port-security** command is the same as the **no debug port-security** command.

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.
	<a href="#">show port-security</a>	Displays port-security settings for an interface or for the switch.

# debug rep

Use the **debug rep** privileged EXEC command to enable debugging of Resilient Ethernet Protocol (REP) functions. Use the **no** form of this command to disable debugging.

**debug rep** {all | bpa-event | bpasm | epasm | error | failure-recovery | lsism | packet | prsm}

**no debug rep** {all | bpa-event | bpasm | epasm | error | failure-recovery | lsism | packet | prsm}

## Syntax Description

<b>all</b>	Display all REP debug messages.
<b>bpa-event</b>	Display blocked port advertisement (BPA) debug messages.
<b>bpasm</b>	Display BPA state machine debug messages.
<b>epasm</b>	Display end port advertisement (EPA) state machine debug messages.
<b>error</b>	Display REP protocol error debug messages.
<b>failure-recovery</b>	Display REP switchover event debug messages.
<b>lsism</b>	Display Link State Layer (LSL) state machine debug messages.
<b>packet</b>	Display protocol PDU debug messages.
<b>prsm</b>	Display REP port role state machine debug messages.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

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

## Usage Guidelines

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

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.
<b>show interfaces rep</b>	Displays REP configuration and status for a specified interface or for all interfaces.

# debug qos-manager

Use the **debug qos-manager** privileged EXEC command to enable debugging of the quality of service (QoS) manager software. Use the **no** form of this command to disable debugging.

```
debug qos-manager {all | event | verbose}
```

```
no debug qos-manager {all | event | verbose}
```

Syntax Description	all	Display all QoS-manager debug messages.
	event	Display QoS-manager related-event debug messages.
	verbose	Display QoS-manager detailed debug messages.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** The **undebg qos-manager** command is the same as the **no debug qos-manager** command.

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

# debug spanning-tree

Use the **debug spanning-tree** privileged EXEC command to enable debugging of spanning-tree activities. Use the **no** form of this command to disable debugging.

```
debug spanning-tree {all | bpdu | bpdu-opt | config | etherchannel | events | exceptions | general
                    | mstp | pvst+ | root | snmp | switch | synchronization}
```

```
no debug spanning-tree {all | bpdu | bpdu-opt | config | etherchannel | events | exceptions |
                       general | mstp | pvst+ | root | snmp | switch | synchronization}
```

Syntax Description		
<b>all</b>	Display all spanning-tree debug messages.	
<b>bpdu</b>	Display spanning-tree bridge protocol data unit (BPDU) debug messages. See the <a href="#">debug spanning-tree bpdu</a> command.	
<b>bpdu-opt</b>	Display optimized BPDU handling debug messages. See the <a href="#">debug spanning-tree bpdu-opt</a> command	
<b>config</b>	Display spanning-tree configuration change debug messages.	
<b>etherchannel</b>	Display EtherChannel-support debug messages.	
<b>events</b>	Display spanning-tree topology event debug messages.	
<b>exceptions</b>	Display spanning-tree exception debug messages.	
<b>general</b>	Display general spanning-tree activity debug messages.	
<b>mstp</b>	Debug Multiple Spanning Tree Protocol events. See the <a href="#">debug spanning-tree mstp</a> command	
<b>pvst+</b>	Display per-VLAN spanning-tree plus (PVST+) event debug messages.	
<b>root</b>	Display spanning-tree root-event debug messages.	
<b>snmp</b>	Display spanning-tree Simple Network Management Protocol (SNMP) handling debug messages.	
<b>switch</b>	Display switch shim command debug messages. This shim is the software module that is the interface between the generic Spanning Tree Protocol (STP) code and the platform-specific code of various switch platforms. See the <a href="#">debug spanning-tree switch</a> command	
<b>synchronization</b>	Display the spanning-tree synchronization event debug messages.	



### Note

Though visible in the command-line help strings, the **backbonefast**, **csuf/csrt**, and **uplinkfast** keywords are not supported.

### Defaults

Debugging is disabled.

### Command Modes

Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** The **undebg spanning-tree** command is the same as the **no debug spanning-tree** command.

Related Commands	Command	Description
	<code>show debugging</code>	Displays information about the types of debugging that are enabled.
	<code>show spanning-tree</code>	Displays spanning-tree state information.

# debug spanning-tree bpdu

Use the **debug spanning-tree bpdu** privileged EXEC command to enable debugging of sent and received spanning-tree bridge protocol data units (BPDUs). Use the **no** form of this command to disable debugging.

**debug spanning-tree bpdu** [receive | transmit]

**no debug spanning-tree bpdu** [receive | transmit]

## Syntax Description

<b>receive</b>	(Optional) Display the nonoptimized path for received BPDU debug messages.
<b>transmit</b>	(Optional) Display the nonoptimized path for sent BPDU debug messages.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The **undebug spanning-tree bpdu** command is the same as the **no debug spanning-tree bpdu** command.

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.
<b>show spanning-tree</b>	Displays spanning-tree state information.

# debug spanning-tree bpdu-opt

Use the **debug spanning-tree bpdu-opt** privileged EXEC command to enable debugging of optimized spanning-tree bridge protocol data units (BPDUs) handling. Use the **no** form of this command to disable debugging.

**debug spanning-tree bpdu-opt [detail | packet]**

**no debug spanning-tree bpdu-opt [detail | packet]**

Syntax Description	detail	(Optional) Display detailed optimized BPDU-handling debug messages.
	packet	(Optional) Display packet-level optimized BPDU-handling debug messages.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** The **undebg spanning-tree bpdu-opt** command is the same as the **no debug spanning-tree bpdu-opt** command.

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.
	<b>show spanning-tree</b>	Displays spanning-tree state information.

## debug spanning-tree mstp

Use the **debug spanning-tree mstp** privileged EXEC command to enable debugging of the Multiple Spanning Tree Protocol (MSTP) software. Use the **no** form of this command to disable debugging.

```
debug spanning-tree mstp {all | boundary | bpdu-rx | bpdu-tx | errors | flush | init | migration |
  pm | proposals | region | roles | sanity_check | sync | tc | timers}
```

```
no debug spanning-tree mstp {all | boundary | bpdu-rx | bpdu-tx | errors | flush | init | migration
  | pm | proposals | region | roles | sanity_check | sync | tc | timers}
```

Syntax Description		
<b>all</b>	Enable all the debugging messages.	
<b>boundary</b>	Debug flag changes at these boundaries:	<ul style="list-style-type: none"> <li>An multiple spanning-tree (MST) region and a single spanning-tree region running Rapid Spanning Tree Protocol (RSTP)</li> <li>An MST region and a single spanning-tree region running IEEE 802.1D</li> <li>An MST region and another MST region with a different configuration</li> </ul>
<b>bpdu-rx</b>	Debug the received MST bridge protocol data units (BPDUs).	
<b>bpdu-tx</b>	Debug the sent MST BPDUs.	
<b>errors</b>	Debug MSTP errors.	
<b>flush</b>	Debug the port flushing mechanism.	
<b>init</b>	Debug the initialization of the MSTP data structures.	
<b>migration</b>	Debug the protocol migration state machine.	
<b>pm</b>	Debug MSTP port manager events.	
<b>proposals</b>	Debug handshake messages between the designated switch and the root switch.	
<b>region</b>	Debug the region synchronization between the switch processor (SP) and the route processor (RP).	
<b>roles</b>	Debug MSTP roles.	
<b>sanity_check</b>	Debug the received BPDU sanity check messages.	
<b>sync</b>	Debug the port synchronization events.	
<b>tc</b>	Debug topology change notification events.	
<b>timers</b>	Debug the MSTP timers for start, stop, and expire events.	

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.



**Usage Guidelines**

The **undebg spanning-tree mstp** command is the same as the **no debug spanning-tree mstp** command.

**Related Commands**

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.
<b>show spanning-tree</b>	Displays spanning-tree state information.

# debug spanning-tree switch

Use the **debug spanning-tree switch** privileged EXEC command to enable debugging of the software interface between the Spanning Tree Protocol (STP) software module and the port manager software module. Use the **no** form of this command to disable debugging.

```
debug spanning-tree switch {all | errors | flush | general | helper | pm | rx {decode | errors |
interrupt | process} | state | tx [decode]}
```

```
no debug spanning-tree switch {all | errors | flush | general | helper | pm | rx {decode | errors |
interrupt | process} | state | tx [decode]}
```

## Syntax Description

<b>all</b>	Display all spanning-tree switch debug messages.
<b>errors</b>	Display debug messages for the interface between the spanning-tree software module and the port manager software module.
<b>flush</b>	Display debug messages for the shim flush operation.
<b>general</b>	Display general event debug messages.
<b>helper</b>	Display spanning-tree helper-task debug messages. Helper tasks handle bulk spanning-tree updates.
<b>pm</b>	Display port-manager event debug messages.
<b>rx</b>	Display received bridge protocol data unit (BPDU) handling debug messages. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>decode</b>—Display decoded received packets.</li> <li>• <b>errors</b>—Display receive error debug messages.</li> <li>• <b>interrupt</b>—Display interrupt service request (ISR) debug messages.</li> <li>• <b>process</b>—Display process receive BPDU debug messages.</li> </ul>
<b>state</b>	Display spanning-tree port state change debug messages;
<b>tx [decode]</b>	Display sent BPDU handling debug messages. The keyword has this meaning: <ul style="list-style-type: none"> <li>• <b>decode</b>—(Optional) Display decoded sent packets.</li> </ul>



## Note

Though visible in the command-line help strings, the **uplinkfast** keyword is not supported.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

**Usage Guidelines**

The **undebg spanning-tree switch** command is the same as the **no debug spanning-tree switch** command.

**Related Commands**

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.
<b>show spanning-tree</b>	Displays spanning-tree state information.

# debug sw-vlan

Use the **debug sw-vlan** privileged EXEC command to enable debugging of VLAN manager activities. Use the **no** form of this command to disable debugging.

```
debug sw-vlan {badpmcookies | cfg-vlan {bootup | cli} | events | ifs | management | notification
| packets | registries}
```

```
no debug sw-vlan {badpmcookies | cfg-vlan {bootup | cli} | events | ifs | management |
notification | packets | registries}
```

Syntax Description		
<b>badpmcookies</b>		Display debug messages for VLAN manager incidents of bad port manager cookies.
<b>cfg-vlan {bootup   cli}</b>		Display config-vlan debug messages. The keywords have these meanings: <ul style="list-style-type: none"> <li><b>bootup</b>—Display messages when the switch is booting up.</li> <li><b>cli</b>—Display messages when the command-line interface (CLI) is in config-vlan mode.</li> </ul>
<b>events</b>		Display debug messages for VLAN manager events.
<b>ifs</b>		See the <a href="#">debug sw-vlan ifs</a> command.
<b>management</b>		Display debug messages for VLAN manager management of internal VLANs.
<b>notification</b>		See the <a href="#">debug sw-vlan notification</a> command.
<b>packets</b>		Display debug messages for packet handling and encapsulation processes.
<b>registries</b>		Display debug messages for VLAN manager registries.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** The **undebug sw-vlan** command is the same as the **no debug sw-vlan** command.

Related Commands	Command	Description
	<a href="#">show debugging</a>	Displays information about the types of debugging that are enabled.
	<a href="#">show vlan</a>	Displays the parameters for all configured VLANs or one VLAN (if the VLAN name or ID is specified) in the administrative domain.

# debug sw-vlan ifs

Use the **debug sw-vlan ifs** privileged EXEC command to enable debugging of the VLAN manager IOS file system (IFS) error tests. Use the **no** form of this command to disable debugging.

```
debug sw-vlan ifs {open {read | write} | read {1 | 2 | 3 | 4} | write}
```

```
no debug sw-vlan ifs {open {read | write} | read {1 | 2 | 3 | 4} | write}
```

## Syntax Description

<b>open {read   write}</b>	Display VLAN manager IFS file-open operation debug messages. The keywords have these meanings: <ul style="list-style-type: none"> <li><b>read</b>—Display VLAN manager IFS file-read operation debug messages.</li> <li><b>write</b>—Display VLAN manager IFS file-write operation debug messages.</li> </ul>
<b>read {1   2   3   4}</b>	Display file-read operation debug messages for the specified error test (1, 2, 3, or 4).
<b>write</b>	Display file-write operation debug messages.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The **undebug sw-vlan ifs** command is the same as the **no debug sw-vlan ifs** command.

When selecting the file read operation, Operation **1** reads the file header, which contains the header verification word and the file version number. Operation **2** reads the main body of the file, which contains most of the domain and VLAN information. Operation **3** reads type length version (TLV) descriptor structures. Operation **4** reads TLV data.

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.
<b>show vlan</b>	Displays the parameters for all configured VLANs or one VLAN (if the VLAN name or ID is specified) in the administrative domain.

# debug sw-vlan notification

Use the **debug sw-vlan notification** privileged EXEC command to enable debugging of the activation and deactivation of VLAN IDs. Use the **no** form of this command to disable debugging.

```
debug sw-vlan notification { accfwdchange | allowedvlanfgchange | fwdchange | linkchange |
modechange | statechange }
```

```
no debug sw-vlan notification { accfwdchange | allowedvlanfgchange | fwdchange |
linkchange | modechange | statechange }
```

## Syntax Description

<b>accfwdchange</b>	Display debug messages for VLAN manager notification of aggregated access interface spanning-tree forward changes.
<b>allowedvlanfgchange</b>	Display debug messages for VLAN manager notification of changes to the allowed VLAN configuration.
<b>fwdchange</b>	Display debug messages for VLAN manager notification of spanning-tree forwarding changes.
<b>linkchange</b>	Display debug messages for VLAN manager notification of interface link-state changes.
<b>modechange</b>	Display debug messages for VLAN manager notification of interface mode changes.
<b>statechange</b>	Display debug messages for VLAN manager notification of interface state changes.



## Note

Though visible in the command-line help strings, the **pruningfgchange** keyword is not supported.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

The **undebug sw-vlan notification** command is the same as the **no debug sw-vlan notification** command.

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.
	<b>show vlan</b>	Displays the parameters for all configured VLANs or one VLAN (if the VLAN name or ID is specified) in the administrative domain.

# debug udd

Use the **debug udd** privileged EXEC command to enable debugging of the UniDirectional Link Detection (UDLD) feature. Use the **no** form of this command to disable UDLD debugging.

**debug udd** { **events** | **packets** | **registries** }

**no debug udd** { **events** | **packets** | **registries** }

## Syntax Description

<b>events</b>	Display debug messages for UDLD process events as they occur.
<b>packets</b>	Display debug messages for the UDLD process as it receives packets from the packet queue and tries to send them at the request of the UDLD protocol code.
<b>registries</b>	Display debug messages for the UDLD process as it processes registry calls from the UDLD process-dependent module and other feature modules.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

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

For **debug udd events**, these debugging messages appear:

- General UDLD program logic flow
- State machine state changes
- Program actions for the set and clear ErrDisable state
- Neighbor cache additions and deletions
- Processing of configuration commands
- Processing of link-up and link-down indications

For **debug udd packets**, these debugging messages appear:

- General packet processing program flow on receipt of an incoming packet
- Indications of the contents of the various pieces of packets received (such as type length versions [TLVs]) as they are examined by the packet reception code
- Packet transmission attempts and the outcome

For **debug udd registries**, these categories of debugging messages appear:

- Sub-block creation
- Fiber-port status changes



- State change indications from the port manager software
- MAC address registry calls

**Related Commands**

Command	Description
<code>show debugging</code>	Displays information about the types of debugging that are enabled.
<code>show udd</code>	Displays UDLD administrative and operational status for all ports or the specified port.

# debug vqpc

Use the **debug vqpc** privileged EXEC command to enable debugging of the VLAN Query Protocol (VQP) client. Use the **no** form of this command to disable debugging.

**debug vqpc** [**all** | **cli** | **events** | **learn** | **packet**]

**no debug vqpc** [**all** | **cli** | **events** | **learn** | **packet**]

## Syntax Description

<b>all</b>	(Optional) Display all VQP client debug messages.
<b>cli</b>	(Optional) Display the VQP client command-line interface (CLI) debug messages.
<b>events</b>	(Optional) Display VQP client event debug messages.
<b>learn</b>	(Optional) Display VQP client address learning debug messages.
<b>packet</b>	(Optional) Display VQP client packet information debug messages.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

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

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.



## APPENDIX **C**

# Cisco ME 3400E Ethernet Access Switch Show Platform Commands

---

This appendix describes the **show platform** privileged EXEC commands that have been created or changed for use with the Cisco ME 3400E Ethernet Access switch. These commands display information helpful in diagnosing and resolving internetworking problems and should be used only under the guidance of Cisco technical support staff.

# show platform acl

Use the **show platform acl** privileged EXEC command to display platform-dependent access control list (ACL) manager information.

```
show platform acl {interface interface-id | label label-number [detail] | statistics asic-number |
usage asic-number [summary] | vlan vlan-id}
```

## Syntax Description

<b>interface</b> <i>interface-id</i>	Display per-interface ACL manager information for the specified interface. The interface can be a physical interface or a VLAN.
<b>label</b> <i>label-number</i> [detail]	Display per-label ACL manager information. The <i>label-number</i> range is 0 to 255. The keyword has this meaning: <ul style="list-style-type: none"> <li><b>detail</b>—(Optional) Display detailed ACL manager label information.</li> </ul>
<b>statistics</b> <i>asic-number</i>	Display per-ASIC ACL statistics. The <i>asic-number</i> is the port ASIC number, always 0.
<b>usage</b> <i>asic-number</i> [summary]	Display per-ASIC ACL usage. The <i>asic-number</i> is the port ASIC number, always 0. The keyword has this meaning: <ul style="list-style-type: none"> <li><b>summary</b>—(Optional) Display brief usage information.</li> </ul>
<b>vlan</b> <i>vlan-id</i>	Display per-VLAN ACL manager information. The <i>vlan-id</i> range is from 1 to 4094.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

# show platform backup interface

Use the **show platform backup interface** privileged EXEC command to display platform-dependent backup information used in a Flex Links configuration.

**show platform backup interface** [*interface-id* | **dummyQ**]

<b>Syntax Description</b>	<i>interface-id</i>	(Optional) Display backup information for all interfaces or the specified interface. The interface can be a physical interface or a port channel.
	<b>dummyQ</b>	(Optional) Display dummy queue information.

**Command Modes** Privileged EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

**Usage Guidelines** You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

# show platform cfm

Use the **show platform cfm** privileged EXEC command to display platform-dependent Ethernet Connectivity Fault Management (CFM) information. CFM is an end-to-end per-service-instance Ethernet layer operation, administration, and management (OAM) protocol that provides proactive connectivity monitoring, fault verification, and fault isolation for large Ethernet networks.

## show platform cfm

**Syntax Description** There are no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

# show platform configuration

Use the **show platform configuration** privileged EXEC command to display platform-dependent configuration-manager related information.

```
show platform configuration { config-output | default | running | startup }
```

Syntax Description	config-output	Display the output of the last auto-configuration application.
	default	Display whether or not the system is running the default configuration.
	running	Display a snapshot of the backed-up running configuration on the local switch.
	startup	Display a snapshot of the backed-up startup configuration on the local switch.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

# show platform dl

Use the **show platform dl** privileged EXEC command to display dynamically loaded module information.

**show platform dl [detail]**

<b>Syntax Description</b>	<b>detail</b> (Optional) Display detailed dynamically loaded module information.
---------------------------	--

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

<b>Usage Guidelines</b>	You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.
-------------------------	--



# show platform etherchannel

Use the **show platform etherchannel** privileged EXEC command to display platform-dependent EtherChannel information.

```
show platform etherchannel {flags | time-stamps}
```

## Syntax Description

<b>flags</b>	Display EtherChannel port flags.
<b>time-stamps</b>	Display EtherChannel time stamps.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

# show platform forward

Use the **show platform forward** privileged EXEC command for an interface to specify how the hardware would forward a frame that matches the specified parameters.

```
show platform forward interface-id [vlan vlan-id] src-mac dst-mac [l3protocol-id] [sap | snap]
[cos cos] [ip src-ip dst-ip] [frag field] [dscp dscp] {l4protocol-id | icmp icmp-type icmp-code |
igmp igmp-version igmp-type | tcp src-port dst-port flags | udp src-port dst-port}
```

Syntax	Description
<i>interface-id</i>	The input physical interface, the port on which the packet comes in to the switch (including type and port number).
<b>vlan</b> <i>vlan-id</i>	(Optional) Input VLAN ID. The range is 1 to 4094. If not specified, and the input interface is not a routed port, the default is 1.
<i>src-mac</i>	48-bit source MAC address.
<i>dst-mac</i>	48-bit destination MAC address.
<i>l3protocol-id</i>	(Optional) The Layer 3 protocol used in the packet. The number is a value 0 to 65535.
<b>sap</b>	(Optional) Service access point (SAP) encapsulation type.
<b>snap</b>	(Optional) Subnetwork Access Protocol (SNAP) encapsulation type.
<b>cos</b> <i>cos</i>	(Optional) Class of service (CoS) value of the frame. The range is 0 to 7.
<b>ip</b> <i>src-ip</i> <i>dst-ip</i>	(Optional, but required for IP packets) Source and destination IP addresses in dotted decimal notation.
<b>frag</b> <i>field</i>	(Optional) The IP fragment field for a fragmented IP packet. The range is 0 to 65535.
<b>dscp</b> <i>dscp</i>	(Optional) Differentiated Services Code Point (DSCP) field in the IP header. The range is 0 to 63.
<i>l4protocol-id</i>	The numeric value of the Layer 4 protocol field in the IP header. The range is 0 to 255. For example, 47 is generic routing encapsulation (GRE), and 89 is Open Shortest Path First (OSPF). If the protocol is TCP, UDP, ICMP, or IGMP, you should use the appropriate keyword instead of a numeric value.
<b>icmp</b> <i>icmp-type</i> <i>icmp-code</i>	Internet Control Message Protocol (ICMP) parameters. The <i>icmp-type</i> and <i>icmp-code</i> ranges are 0 to 255.
<b>igmp</b> <i>igmp-version</i> <i>igmp-type</i>	Internet Group Management Protocol (IGMP) parameters. The <i>igmp-version</i> range is 1 to 15; the <i>igmp-type</i> range is 0 to 15.
<b>tcp</b> <i>src-port</i> <i>dst-port</i> <i>flags</i>	TCP parameters: TCP source port, destination port, and the numeric value of the TCP flags byte in the header. The <i>src-port</i> and <i>dst-port</i> ranges are 0 to 65535. The flag range is from 0 to 1024.
<b>udp</b> <i>src-port</i> <i>dst-port</i>	User Datagram Protocol (UDP) parameters. The <i>src-port</i> and <i>dst-port</i> ranges are 0 to 65535.



## Note

Though visible in the command-line help strings, the **ipv6** keyword is not supported.

---

**Command Modes** Privileged EXEC

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

---

---

**Usage Guidelines** You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

---

**Examples** See the “Troubleshooting” chapter of the software configuration guide for this release for examples of the **show platform forward** command output displays and what they mean.

# show platform frontend-controller

Use the **show platform frontend-controller** privileged EXEC command to display counter and status information for the front-end controller manager and subordinate applications and to display the hardware and software information for the front-end controller.

```
show platform frontend-controller {buffer | generic | manager number | subordinate number |
version number}
```

Syntax Description		
<b>buffer</b>		Display the last 1024 bytes sent from the manager to the subordinate and the reverse.
<b>generic</b>		Display the generic counters that do not specifically apply to the manager or subordinate.
<b>manager <i>number</i></b>		Display the counters for the manager and the subordinate specified by <i>number</i> . See the “Usage Guidelines” section for the <i>number</i> range.
<b>subordinate <i>number</i></b>		Display the subordinate status and the counters for the subordinate specified by <i>number</i> . See the “Usage Guidelines” section for the <i>number</i> range.
<b>version <i>number</i></b>		Display the hardware and software version information for the subordinate status specified by <i>number</i> . The range is from 0 to 1.

Command Modes	
	Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

Usage Guidelines	
	You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

# show platform ip igmp snooping

Use the **show platform ip igmp snooping** privileged EXEC command to display platform-dependent Internet Group Management Protocol (IGMP) snooping information.

```
show platform ip igmp snooping {all | control [di] | counters | flood [vlan vlan-id] | group
ip-address | hardware | retry [count | local [count] | remote [count]]}
```

Syntax Description	
<b>all</b>	Display all IGMP snooping platform IP multicast information.
<b>control [di]</b>	Display IGMP snooping control entries. The keyword has this meaning: <ul style="list-style-type: none"> <li><b>di</b>—(Optional) Display IGMP snooping control destination index entries.</li> </ul>
<b>counters</b>	Display IGMP snooping counters.
<b>flood [vlan <i>vlan-id</i>]</b>	Display IGMP snooping flood information. The keyword has this meaning: <ul style="list-style-type: none"> <li><b>vlan <i>vlan-id</i></b>—(Optional) Display flood information for the specified VLAN. The range is 1 to 4094.</li> </ul>
<b>group <i>ip-address</i></b>	Display the IGMP snooping multicast group information, where <i>ip-address</i> is the IP address of the group.
<b>hardware</b>	Display IGMP snooping information loaded into hardware.
<b>retry [count   local [count]   remote [count]]</b>	Display IGMP snooping retry information. The keywords have these meanings: <ul style="list-style-type: none"> <li><b>count</b>—(Optional) Display only the retry count.</li> <li><b>local</b>—(Optional) Display local retry entries.</li> </ul>
<b>remote [count]</b>	Display remote entries. The keyword has this meaning: <ul style="list-style-type: none"> <li><b>count</b>—(Optional) Display only the remote count.</li> </ul>

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

# show platform ip multicast

Use the **show platform ip multicast** privileged EXEC command to display platform-dependent IP multicast tables and other information.

```
show platform ip multicast {acl-full-info | counters | groups | hardware [detail] | interfaces |
locks | mdfs-routes | retry | trace}
```

Syntax Description		
<b>acl-full-info</b>		Display IP multicast routing access-control list (ACL) information, in particular the number of outgoing VLANs for which router ACLs at the output cannot be applied in hardware.
<b>counters</b>		Display IP multicast counters and statistics.
<b>groups</b>		Display IP multicast routes per group.
<b>hardware [detail]</b>		Display IP multicast routes loaded into hardware. The optional <b>detail</b> keyword is used to show port members in the destination index and route index.
<b>interfaces</b>		Display IP multicast interfaces.
<b>locks</b>		Display IP multicast destination-index locks.
<b>mdfs-routes</b>		Display multicast distributed fast switching (MDFS) IP multicast routes.
<b>retry</b>		Display the IP multicast routes in the retry queue.
<b>trace</b>		Display the IP multicast trace buffer.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

# show platform ip unicast

Use the **show platform ip unicast** privileged EXEC command to display platform-dependent IP unicast routing information.

```
show platform ip unicast { adjacency | cef-idb | counts | dhcp | failed { adjacency | arp [A.B.C.D]
| route } | loadbalance | mpaths | route | standby | statistics | trace }
```

Syntax Description	
<b>adjacency</b>	Display the platform adjacency database.
<b>cef-idb</b>	Display platform information corresponding to Cisco Express Forwarding (CEF) interface descriptor block.
<b>counts</b>	Display the current counts for the Layer 3 unicast databases.
<b>dhcp</b>	Display the DHCP system dynamic addresses.
<b>failed { adjacency   arp [A.B.C.D]   route }</b>	Display the hardware resource failures. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>adjacency</b>—Display the adjacency entries that failed to be programmed in hardware.</li> <li>• <b>arp</b>—Display the Address Resolution Protocol (ARP) deletions because of failure and because of retries.</li> <li>• <i>A.B.C.D</i>—(Optional) Prefix of the ARP entries to display.</li> <li>• <b>route</b>—Display the route entries that failed to be programmed in hardware.</li> </ul>
<b>loadbalance</b>	Display the platform load balancing database.
<b>mpaths</b>	Display the Layer 3 unicast routing multipath adjacency database.
<b>route</b>	Display the platform route database.
<b>standby</b>	Display the platform standby information.
<b>statistics</b>	Display the Layer 3 unicast routing accumulated statistics.
<b>trace</b>	Display the platform event trace logs.



## Note

Though visible in the command-line help strings, the **proxy** and **table** keywords are not supported.

Command Modes	
	Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

# show platform ipc trace

Use the **show platform ipc trace** privileged EXEC command to display platform-dependent Interprocess Communication (IPC) Protocol trace log information.

**show platform ipc trace**

**Syntax Description** There are no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.



# show platform ipv6 unicast

Use the **show platform ipv6 unicast** privileged EXEC command to display platform-dependent IPv6 unicast routing information.

```
show platform ipv6 unicast { adjacency [ipv6-prefix] | backwalk { adjacency | loadbalance } |
compress ipv6-prefix/prefix length | interface | loadbalance | mpath | retry { adjacency |
route } | route [ipv6-prefix/prefix length | tcam] [detail] | statistics | table [detail] | trace }
```



## Note

This command is available only if the switch is running the metro IP access image and you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

## Syntax Description

<b>adjacency</b>	Display IPv6 adjacency information for the switch or for the specified IPv6 network.
<i>ipv6-prefix</i>	(Optional) The IPv6 network to be displayed. The address must be specified in hexadecimal using 16-bit values between colons.
<b>backwalk { adjacency   loadbalance }</b>	Display IPv6 backwalk information. <ul style="list-style-type: none"> <li><b>adjacency</b>—Display adjacency backwalk information.</li> <li><b>loadbalance</b>—Display backwalk load-balance information.</li> </ul>
<b>compress</b> <i>ipv6-prefix/prefix length</i>	Display IPv6 prefix compression information. <ul style="list-style-type: none"> <li><i>ipv6-prefix</i>—The IPv6 network.</li> <li><i>/prefix length</i>—The length of the IPv6 network prefix. A decimal value from 0 to 128 that shows how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.</li> </ul>
<b>interface</b>	Display IPv6 interface information.
<b>loadbalance</b>	Display IPv6 load-balance information
<b>mpath</b>	Display IPv6 multipath information
<b>retry { adjacency   route }</b>	Display IPv6 retry information. <ul style="list-style-type: none"> <li><b>adjacency</b>—Display IPv6 adjacency retry information.</li> <li><b>route</b>—Display IPv6 route retry information.</li> </ul>
<b>route</b>	Display IPv6 route information.
<b>tcam</b>	(Optional) Display the IPv6 hardware route table information.
<b>detail</b>	(Optional) Display detailed IPv6 route information.
<b>statistics</b>	Display IPv6 accumulated statistics.
<b>table</b>	Display IPv6 unicast table information.
<b>trace</b>	Display IPv6 unicast traces.

## Command Modes

Privileged EXEC

**show platform ipv6 unicast****Command History**

<b>Release</b>	<b>Modification</b>
12.2(50)SE	This command was introduced.

**Usage Guidelines**

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

# show platform l2pt dm

Use the **show platform l2pt dm** privileged EXEC command to display Layer 2 protocol tunneling destination maps and associated ports.

**show platform l2pt dm**

---

**Syntax Description** There are no arguments or keywords.

---

**Command Modes** Privileged EXEC

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

---

---

**Usage Guidelines** You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

# show platform layer4op

Use the **show platform layer4op** privileged EXEC command to display platform-dependent Layer 4 operator information.

```
show platform layer4op {acl | qos [port-asic]} {and-or | map | or-and | vcu}
```

Syntax Description	Parameter	Description
	<b>acl</b>	Display access control list (ACL) Layer 4 operators information.
	<b>qos</b> [ <i>port-asic</i> ]	Display quality of service (QoS) Layer 4 operators information. The keyword has this meaning: <ul style="list-style-type: none"> <li><i>port-asic</i>—(Optional) QoS port ASIC number. The value can be 0 or 1.</li> </ul>
	<b>and-or</b>	Display AND-OR registers information.
	<b>map</b>	Display select map information.
	<b>or-and</b>	Display OR-AND registers information.
	<b>vcu</b>	Display value compare unit (VCU) register information.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

# show platform mac-address-table

Use the **show platform mac-address-table** privileged EXEC command to display platform-dependent MAC address table information.

```
show platform mac-address-table [aging-array | hash-table | mac-address mac-address] [vlan
vlan-id]
```

Syntax Description	
<b>aging-array</b>	(Optional) Display the MAC address table aging array.
<b>hash-table</b>	(Optional) Display the MAC address table hash table.
<b>mac-address</b> <i>mac-address</i>	(Optional) Display the MAC address table MAC address information, where <i>mac-address</i> is the 48-bit hardware address.
<b>vlan</b> <i>vlan-id</i>	(Optional) Display information for the specified VLAN. The range is 1 to 4094.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

# show platform messaging

Use the **show platform messaging** privileged EXEC command to display platform-dependent application and performance message information.

```
show platform messaging {application [incoming | outgoing | summary] | hipperf
                        [class-number]}
```

## Syntax Description

<b>application</b> [incoming   outgoing   summary]	Display application message information. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>incoming</b>—(Optional) Display only information about incoming application messaging requests.</li> <li>• <b>outgoing</b>—(Optional) Display only information about incoming application messaging requests.</li> <li>• <b>summary</b>—(Optional) Display summary information about all application messaging requests.</li> </ul>
<b>hipperf</b> [class-number]	Display outgoing high-performance message information. Specify the <i>class-number</i> option to display information about high-performance messages for this class number. The range is 0 to 36.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

# show platform monitor

Use the **show platform monitor** privileged EXEC command to display platform-dependent Switched Port Analyzer (SPAN) information.

**show platform monitor** [**session** *session-number*]

<b>Syntax Description</b>	<b>session</b> <i>session-number</i>	(Optional) Display SPAN information for the specified SPAN session. The range is 1 to 66.
---------------------------	---	---

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

<b>Usage Guidelines</b>	You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.
-------------------------	--

## show platform mvr table

Use the **show platform mvr table** privileged EXEC command to display the platform-dependent Multicast VLAN Registration (MVR) multi-expansion descriptor (MED) group mapping table.

### show platform mvr table

**Syntax Description** There are no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.



# show platform pm

Use the **show platform pm** privileged EXEC command to display platform-dependent port-manager information.

```
show platform pm { counters | group-masks | idbs { active-idbs | deleted-idbs } | if-numbers |
link-status | platform-block | port-info interface-id | vlan { info | line-state }
```

Syntax Description		
<b>counters</b>		Display module counters information.
<b>group-masks</b>		Display EtherChannel group masks information.
<b>idbs { active-idbs   deleted-idbs }</b>		Display interface data block (IDB) information. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>active-idbs</b>—Display active IDB information.</li> <li>• <b>deleted-idbs</b>—Display deleted and leaked IDB information.</li> </ul>
<b>if-numbers</b>		Display interface numbers information.
<b>link-status</b>		Display local port link status information.
<b>platform-block</b>		Display platform port block information.
<b>port-info</b> <i>interface-id</i>		Display port administrative and operation fields for the specified interface.
<b>vlan { info   line-state }</b>		Display platform VLAN information. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>info</b>—Display information for active VLANs.</li> <li>• <b>line-state</b>—Display line-state information.</li> </ul>



## Note

Though visible in the command-line help strings, the **stack-view** keyword is not supported.

Command Modes	
	Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

# show platform policer cpu

Use the **show platform policer cpu** privileged EXEC command to display CPU control-plane policer statistics per feature or the indexes and the corresponding feature for the specified port.

**show platform policer cpu** { **classification** | **interface** *interface-id* }

## Syntax Description

<b>classification</b>	Displays policer statistics per feature.
<b>interface</b> <i>interface-id</i>	Display the policer indexes for a specific interface.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

For CPU protection of user network interfaces (UNIs) and enhanced network interfaces (ENIs), the switch pre-allocates the 27 CPU protection policers, numbered 0 to 26. On the ME 3400E-24TS switch, a policer of 26 means a drop policer; any traffic type shown as 26 on any port is dropped. A policer of a value of 0 to 25 means that a rate-limiting policer is assigned to the port for the control protocol. A policer value of 255 means that no policer is assigned to a control protocol. Network node interfaces (NNIs) have no policers assigned.

For the ME 3400EG-12CS and ME 3400EG-2CS switches, a policer of 4 means a drop policer. A traffic type shown as 4 on a port is dropped. A policer value of 0 to 3 means that a rate-limiting policer is assigned to the port for the protocol.

## Examples

This is an example of output from the **show platform policer cpu classification** command:



### Note

Unless otherwise indicated, the examples are for an ME 3400E-24TS switch.

```
Switch# show platform policer cpu classification
=====
SWITCH 1
=====
Feature                Bytes          Frames
=====
STP                    3912792        61278
LACP                   0              0
8021X                  0              0
RSVD_STP               0              0
PVST_PLUS              0              0
CDP                    1012542        2552
DTP                    131264         2051
UDLD                   0              0
PAGP                   0              0
```

```

VTP                                0                0
CISCO_L2                           0                0
KEEPALIVE                          0                0
CFM                                 0                0
SWITCH_MAC                          0                0
SWITCH_ROUTER_MAC                  896              14
SWITCH_IGMP                        289408           4522
SWITCH_L2PT                         0                0

```

This example of the output from the **show platform policer cpu interface** command shows the default policer configuration for a UNI. Because the port is Fast Ethernet 1, the identifier for rate-limited protocols is 0; a display for Fast Ethernet port 5 would display an identifier of 4. The *Policer Index* refers to the specific protocol. The ASIC number indicates when the policer is on a different ASIC.

Because UNIs do not support STP, CDP, LLDP, LACP, and PAGP, these packets are dropped (physical policer of 26). These protocols are disabled by default on ENIs as well, but you can enable them. When enabled on ENIs, the control packets are rate-limited and a rate-limiting policers is assigned to the port for these protocols (physical policer of 22).

```

Switch# show platform policer cpu interface fastethernet 0/3
Policers assigned for CPU protection
=====
Feature                               Policer          Physical        Asic
Index                                Policer          Num
=====
Fa0/1
STP                                   1                26              0
LACP                                  2                26              0
8021X                                 3                26              0
RSVD_STP                              4                26              0
PVST_PLUS                             5                26              0
CDP                                    6                26              0
LLDP                                  7                26              0
DTP                                   8                26              0
UDLD                                  9                26              0
PAGP                                  10               26              0
VTP                                   11               26              0
CISCO_L2                              12               26              0
KEEPALIVE                             13               0                0
CFM                                    14               255              0
SWITCH_MAC                             15               26              0
SWITCH_ROUTER_MAC                     16               26              0
SWITCH_IGMP                           17               0                0
SWITCH_L2PT                           18               26              0

```

This example shows the policers assigned to a ENI when control protocols are enabled on the interface. A value of 22 indicates that protocol packets are rate-limited for that protocol. When the protocol is not enabled, the defaults are the same as for a UNI.

```

Switch# show platform policer cpu interface fastethernet0/23
Policers assigned for CPU protection
=====
Feature                               Policer          Physical        Asic
Index                                Policer          Num
=====
Fa0/23
STP                                   1                26              0
LACP                                  2                22              0
8021X                                 3                26              0
RSVD_STP                              4                26              0
PVST_PLUS                             5                26              0
CDP                                    6                22              0
LLDP                                  7                26              0

```

## show platform policer cpu

DTP	8	26	0
UDLD	9	26	0
PAGP	10	26	0
VTP	11	26	0
CISCO_L2	12	22	0
KEEPALIVE	13	22	0
CFM	14	255	0
SWITCH_MAC	15	26	0
SWITCH_ROUTER_MAC	16	26	0
SWITCH_IGMP	17	22	0
SWITCH_L2PT	18	22	0

This example shows rate limiting on a ME 3400EG-12CS or ME 3400EG-2CS switch. A value of 1 shows that protocol packets are rate limited for that protocol.

Switch #**show platform policer cpu interface gigabitethernet 0/2**  
Policers assigned for CPU protection

```
=====
```

Feature	Policer Index	Physical Policer	Asic Num
=====			
Gi0/2			
STP	1	4	0
LACP	2	4	0
8021X	3	4	0
RSVD_STP	4	1	0
PVST_PLUS	5	4	0
CDP	6	4	0
LLDP	7	4	0
DTP	8	4	0
UDLD	9	4	0
PAGP	10	4	0
VTP	11	4	0
CISCO_L2	12	4	0
KEEPALIVE	13	1	0
CFM	14	255	0
SWITCH_MAC	15	4	0
SWITCH_ROUTER_MAC	16	4	0
SWITCH_IGMP	17	1	0
SWITCH_L2PT	18	4	0

```
=====
```

This example shows the default policers assigned to NNIs. Most protocols have no policers assigned to NNIs. A value of 255 means that no policer is assigned to the port for the protocol.

Switch #**show platform policer cpu interface gigabitethernet 0/1**  
Policers assigned for CPU protection

```
=====
```

Feature	Policer Index	Physical Policer	Asic Num
=====			
Gi0/1			
STP	1	255	0
LACP	2	255	0
8021X	3	255	0
RSVD_STP	4	255	0
PVST_PLUS	5	255	0
CDP	6	255	0
LLDP	7	255	0
DTP	8	255	0
UDLD	9	255	0
PAGP	10	255	0
VTP	11	255	0
CISCO_L2	12	255	0
KEEPALIVE	13	255	0

```
=====
```

CFM	14	255	0
SWITCH_MAC	15	255	0
SWITCH_ROUTER_MAC	16	255	0
SWITCH_IGMP	17	255	0
SWITCH_L2PT	18	255	0

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">show policer cpu uni-eni</a>	Displays control-plane policer information for the switch.

## show platform port-asic

Use the **show platform port-asic** privileged EXEC command to display platform-dependent port application-specific integrated circuit (ASIC) register information.

```
show platform port-asic {cpu-queue-map-table [asic number | port number [asic number]] |
  dest-map index number | etherchannel-info [asic number | port number [asic number]] |
  exception [asic number | port number [asic number]] | global-status [asic number |
  port number [asic number]] | learning [asic number | port number [asic number]] |
  mac-info [asic number | port number [asic number]] | mvid [asic number] |
  packet-info-ram [asic number | index number [asic number]] |
  port-info [asic number | port number [asic number]] |
  prog-parser [asic number | port number [asic number]] |
  receive {buffer-queue | port-fifo | supervisor-sram} [asic number | port number [asic
  number]] | span [vlan-id [asic number] | [asic number]
  stats {drop | enqueue | miscellaneous | supervisor} [asic number | port number [asic
  number]] |
  transmit {port-fifo | queue | supervisor-sram} [asic number | port number [asic number]]
  vct [asic number | port number [asic number]]}
```

### Syntax Description

<b>cpu-queue-map-table</b> [asic number   port number [asic number]]	Display the CPU queue-map table entries. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The range is 0 to 1.</li> <li>• <b>port number</b>—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27.</li> </ul>
<b>dest-map index</b> number	Display destination-map information for the specified index. The range is 0 to 65535.
<b>etherchannel-info</b> [asic number   port number [asic number]]	Display the contents of the EtherChannel information register. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The number is always 0.</li> <li>• <b>port number</b>—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.</li> </ul>
<b>exception</b> [asic number   port number [asic number]]	Display the exception-index register information. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The number is always 0.</li> <li>• <b>port number</b>—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.</li> </ul>

<b>global-status</b> [ <i>asic number</i>   <i>port number</i> [ <i>asic number</i> ]]	<p>Display global and interrupt status. The keywords have these meanings:</p> <ul style="list-style-type: none"> <li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The number is always 0.</li> <li>• <b>port number</b>—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.</li> </ul>
<b>learning</b> [ <i>asic number</i>   <i>port number</i> [ <i>asic number</i> ]]	<p>Display entries in the learning cache. The keywords have these meanings:</p> <ul style="list-style-type: none"> <li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The number is always 0.</li> <li>• <b>port number</b>—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.</li> </ul>
<b>mac-info</b> [ <i>asic number</i>   <i>port number</i> [ <i>asic number</i> ]]	<p>Display the contents of the MAC information register. The keywords have these meanings:</p> <ul style="list-style-type: none"> <li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The number is always 0.</li> <li>• <b>port number</b>—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.</li> </ul>
<b>mvid</b> [ <i>asic number</i> ]	<p>Display the mapped VLAN ID table. The keyword has this meaning:</p> <ul style="list-style-type: none"> <li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The number is always 0.</li> </ul>
<b>packet-info-ram</b> [ <i>asic number</i>   <i>index number</i> [ <i>asic number</i> ]]	<p>Display the packet information RAM. The keywords have these meanings:</p> <ul style="list-style-type: none"> <li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The number is always 0.</li> <li>• <b>index number</b>—(Optional) Display information for the specified packet RAM index number and ASIC number. The range is 0 to 63.</li> </ul>
<b>port-info</b> [ <i>asic number</i>   <i>port number</i> [ <i>asic number</i> ]]	<p>Display port information register values. The keywords have these meanings:</p> <ul style="list-style-type: none"> <li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The number is always 0.</li> <li>• <b>port number</b>—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.</li> </ul>

<b>prog-parser</b> [ <b>asic number</b>   <b>port number</b> [ <b>asic number</b> ]]	<p>Display the programmable parser tables. The keywords have these meanings:</p> <ul style="list-style-type: none"> <li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The number is always 0.</li> <li>• <b>port number</b>—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.</li> </ul>
<b>receive</b> { <b>buffer-queue</b>   <b>port-fifo</b>   <b>supervisor-sram</b> } [ <b>asic number</b>   <b>port number</b> [ <b>asic number</b> ]]	<p>Display receive information. The keywords have these meanings:</p> <ul style="list-style-type: none"> <li>• <b>buffer-queue</b>—Display the buffer queue information.</li> <li>• <b>port-fifo</b>—Display the port-FIFO information.</li> <li>• <b>supervisor-sram</b>—Display the supervisor static RAM (SRAM) information.</li> <li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The number is always 0.</li> <li>• <b>port number</b>—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.</li> </ul>
<b>span</b> [ <b>vlan-id</b>   <b>asic number</b> ]	<p>Display the Switched Port Analyzer (SPAN)-related information. The keywords have these meanings:</p> <ul style="list-style-type: none"> <li>• <b>vlan-id</b>—(Optional) Display information for the specified VLAN. The range is 0 to 1023.</li> <li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The number is always 0.</li> </ul>
<b>stats</b> { <b>drop</b>   <b>enqueue</b>   <b>miscellaneous</b>   <b>supervisor</b> } [ <b>asic number</b>   <b>port number</b> [ <b>asic number</b> ]]	<p>Display raw statistics for the port ASIC. The keywords have these meanings:</p> <ul style="list-style-type: none"> <li>• <b>drop</b>—Display drop statistics.</li> <li>• <b>enqueue</b>—Display enqueue statistics.</li> <li>• <b>miscellaneous</b>—Display miscellaneous statistics.</li> <li>• <b>supervisor</b>—Display supervisor statistics.</li> <li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The number is always 0.</li> <li>• <b>port number</b>—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.</li> </ul>



<b>transmit</b> { <b>port-fifo</b>   <b>queue</b>   <b>supervisor-sram</b> } [ <b>asic number</b>   <b>port number</b> [ <b>asic number</b> ]]	<p>Display transmit information. The keywords have these meanings:</p> <ul style="list-style-type: none"> <li>• <b>port-fifo</b>—Display the contents of the port-FIFO information register.</li> <li>• <b>queue</b>—Display the contents of the queue information register.</li> <li>• <b>supervisor-sram</b>—Display supervisor SRAM information.</li> <li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The range is 0 to 1.</li> <li>• <b>port number</b>—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.</li> </ul>
<b>vct</b> [ <b>asic number</b>   <b>port number</b> [ <b>asic number</b> ]]	<p>Display the VLAN compression table entries for the specified ASIC or for the specified port and ASIC. The keywords have these meanings:</p> <ul style="list-style-type: none"> <li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The range is 0 to 1.</li> <li>• <b>port number</b>—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.</li> </ul>

**Note**

Though visible in the command-line help strings, the **stack** { **control** | **dest-map** | **learning** | **messages** | **mvid** | **prog-parser** | **span** | **stats** [**asic number** | **port number** [**asic number**]] keywords are not supported.

**Command Modes**

Privileged EXEC

**Command History**

Release	Modification
12.2(44)EY	This command was introduced.

**Usage Guidelines**

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

# show platform port-security

Use the **show platform port-security** privileged EXEC command to display platform-dependent port-security information.

**show platform port-security**

**Syntax Description** There are no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

# show platform qos

Use the **show platform qos** privileged EXEC command to display platform-dependent quality of service (QoS) information.

```
show platform qos debug [aggregate-policer aggregate-policer-name | global-config |
input-queue | [interface interface-id] [buffers | policers | queuing]] | label-table
[dynamic-label { dscp value cos value | label-number value | policy-map policy-map-name
class-map class-map-name } [asic number] | policer { parameter-table | qos-table |
selection-table } [asic number] | policy-map policy-map-name [asic number] | port-class [asic
number] | port-config port-number [asic number] | port-info port-number [asic number] |
table-map | vlan vlan-id]
```

```
show platform qos statistics [interface interface-id]
```

Syntax	Description
<b>debug</b>	Display QoS debug messages for the switch or for the specified keyword.
<b>aggregate-policer</b> <i>aggregate-policer-name</i>	(Optional) Display QoS aggregate policer information for the specified aggregate policer.
<b>global-config</b>	(Optional) Display QoS global configuration information.
<b>input-queue</b>	(Optional) Display QoS input queue information.
<b>interface</b> [ <i>interface-id</i> ] [ <b>buffers</b>   <b>policers</b>   <b>queuing</b> ]	(Optional) Display QoS information for all interfaces or the specified interface. The keywords have these meanings: <ul style="list-style-type: none"> <li><b>buffers</b>—(Optional) Display information about QoS buffers.</li> <li><b>policers</b>—(Optional) Display information about QoS policers.</li> <li><b>queuing</b>—(Optional) Display information about QoS output queues.</li> </ul>
<b>label-table</b> [ <b>dynamic-label</b> { <b>dscp</b> <i>value</i> <b>cos</b> <i>value</i>   <b>label-number</b> <i>value</i>   <b>policy-map</b> <i>policy-map-name</i> <b>class-map</b> <i>class-map-name</i> } [ <b>asic</b> <i>number</i> ]	(Optional) Display QoS label table information. The keywords have these meanings: <ul style="list-style-type: none"> <li><b>dynamic-label</b>—(Optional) Display dynamic label information.</li> <li><b>dscp</b> <i>value</i> <b>cos</b> <i>value</i>—Display information based on Differentiated Services Code Point (DSCP) value (0 to 63) and class of service (CoS) value (0 to 7).</li> <li><b>label-number</b> <i>value</i>—Display information based on the dynamic label number. The range is from 158 to 255.</li> <li><b>policy-map</b> <i>policy-map-name</i> <b>class-map</b> <i>class-map-name</i>—Display information for the specified policy map and class map.</li> <li><b>asic</b> <i>number</i>—(Optional) Display information based on the port ASIC number. The number is always 0.</li> </ul>

<b>policer</b> { <b>parameter-table</b>   <b>qos-table</b>   <b>selection-table</b> } [ <b>asic number</b> ]	(Optional) Display QoS policer information. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>parameter-table</b>—Display the policer parameter table.</li> <li>• <b>qos-table</b>—Display the policer QoS table.</li> <li>• <b>selection-table</b>—Display the port allocation table.</li> <li>• <b>asic number</b>—(Optional) Display information based on the port ASIC number. The number is always 0.</li> </ul>
<b>policy-map</b> <i>policy-map-name</i> [ <b>asic number</b> ]	(Optional) Display QoS information for the specified policy map. <ul style="list-style-type: none"> <li>• <b>asic number</b>—(Optional) Display information based on the port ASIC number. The number is always 0.</li> </ul>
<b>port-class</b> [ <b>asic number</b> ]	(Optional) Display QoS port class tables. <ul style="list-style-type: none"> <li>• <b>asic number</b>—(Optional) Display information based on the port ASIC number. The number is always 0.</li> </ul>
<b>port-config</b> <i>port-number</i> [ <b>asic number</b> ]	(Optional) Display QoS port configuration information. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <i>port-number</i>—Display QoS configuration for the specified port number. The range is 0 to 25.</li> <li>• <b>asic number</b>—(Optional) Display information based on the port ASIC number. The number is always 0.</li> </ul>
<b>port-info</b> <i>port-number</i> [ <b>asic number</b> ]	(Optional) Display QoS port information. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <i>port-number</i>—Display QoS configuration for the specified port number. The range is 0 to 25.</li> <li>• <b>asic number</b>—(Optional) Display information based on the port ASIC number. The number is always 0.</li> </ul>
<b>table-map</b> <i>table-map-name</i> [ <b>asic number</b> ]	(Optional) Display QoS information for the specified table map. <ul style="list-style-type: none"> <li>• <b>asic number</b>—(Optional) Display information based on the port ASIC number. The number is always 0.</li> </ul>
<b>vlan</b> <i>vlan-id</i>	(Optional) Display QoS information for the specified VLAN. The range is 1 to 4094.
<b>statistics</b>	Display QoS interface statistics.

**Command Modes**

Privileged EXEC

**Command History**

Release	Modification
12.2(44)EY	This command was introduced.

**Usage Guidelines**

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

# show platform resource-manager

Use the **show platform resource-manager** privileged EXEC command to display platform-dependent resource-manager information.

```
show platform resource-manager { dm [index number] | erd [index number] |
  mad [index number] | med [index number] | mod | msm { hash-table [vlan vlan-id] |
  mac-address mac-address [vlan vlan-id] } | sd [index number] | vld [index number] }
```

## Syntax Description

<b>dm</b> [index number]	Display the destination map. The keyword has this meaning: <ul style="list-style-type: none"> <li><b>index number</b>—(Optional) Display the specified index. The range is 0 to 65535.</li> </ul>
<b>erd</b> [index number]	Display the equal-cost-route descriptor table for the specified index. The keyword has this meaning: <ul style="list-style-type: none"> <li><b>index number</b>—(Optional) Display the specified index. The range is 0 to 65535.</li> </ul>
<b>mad</b> [index number]	Display the MAC-address descriptor table for the specified index. The keyword has this meaning: <ul style="list-style-type: none"> <li><b>index number</b>—(Optional) Display the specified index. The range is 0 to 65535.</li> </ul>
<b>med</b> [index number]	Display the multi-expansion descriptor table for the specified index. The keyword has this meaning: <ul style="list-style-type: none"> <li><b>index number</b>—(Optional) Display the specified index. The range is 0 to 65535.</li> </ul>
<b>mod</b>	Display the resource-manager module information.
<b>msm</b> { hash-table [vlan vlan-id]   mac-address mac-address [vlan vlan-id] }	Display the MAC-address station descriptor table. The keywords have these meanings: <ul style="list-style-type: none"> <li><b>hash-table</b>—Display the msm hash table.</li> <li><b>mac-address mac-address</b>—Display the table for the specified MAC address.</li> <li><b>vlan vlan-id</b>—(Optional) Display the table for the specified VLAN. The range is 1 to 4094.</li> </ul>
<b>sd</b> [index number]	Display the station descriptor table for the specified index. The keyword has this meaning: <ul style="list-style-type: none"> <li><b>index number</b>—(Optional) Display the specified index. The range is 0 to 65535.</li> </ul>
<b>vld</b> [index number]	Display the VLAN-list descriptor table for the specified index. The keyword has this meaning: <ul style="list-style-type: none"> <li><b>index number</b>—(Optional) Display the specified index. The range is 0 to 65535.</li> </ul>

## Command Modes

Privileged EXEC

**Command History**

<b>Release</b>	<b>Modification</b>
12.2(44)EY	This command was introduced.

**Usage Guidelines**

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

# show platform snmp counters

Use the **show platform snmp counters** privileged EXEC command to display platform-dependent Simple Network Management Protocol (SNMP) counter information.

**show platform snmp counters**

**Syntax Description** There are no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.



# show platform spanning-tree synchronization

Use the **show platform spanning-tree synchronization** privileged EXEC command to display platform-dependent spanning-tree state synchronization information.

**show platform spanning-tree synchronization** [**detail** | **vlan** *vlan-id*]

Syntax Description	detail	(Optional) Display detailed spanning-tree synchronization information.
	<b>vlan</b> <i>vlan-id</i>	(Optional) Display spanning-tree synchronization information for the specified VLAN. The range is 1 to 4094.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

# show platform status

Use the **show platform status** privileged EXEC command to display platform-dependent status information.

**show platform status**

**Syntax Description** There are no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

# show platform stp-instance

Use the **show platform stp-instance** privileged EXEC command to display platform-dependent spanning-tree instance information.

**show platform stp-instance** *vlan-id*

<b>Syntax Description</b>	<i>vlan-id</i>	Display spanning-tree instance information for the specified VLAN. The range is 1 to 4094.
---------------------------	----------------	--

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EY	This command was introduced.

<b>Usage Guidelines</b>	You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.
-------------------------	--

# show platform tcam

Use the **show platform tcam** privileged EXEC command to display platform-dependent ternary content addressable memory (TCAM) driver information.

```

show platform tcam { handle number | log-results | table { acl | all | equal-cost-route | local |
mac-address | multicast-expansion | qos | secondary | station | vlan-list } | usage } [ asic
number [ detail [ invalid ] ] | [ index number [ detail [ invalid ] ] | invalid | num number [ detail
[ invalid ] ] | invalid ] | [ invalid ] | [ num number [ detail [ invalid ] ] | invalid ] ]

show platform tcam table acl [ asic number [ detail [ invalid ] ] | [ index number [ detail [ invalid ] ] |
invalid | num number [ detail [ invalid ] ] | invalid ] | [ invalid ] | [ num number [ detail [ invalid ] ]
| invalid ] ]

show platform tcam table all [ asic number [ detail [ invalid ] ] | [ index number [ detail [ invalid ] ] |
invalid | num number [ detail [ invalid ] ] | invalid ] | [ invalid ] | [ num number [ detail [ invalid ] ]
| invalid ] ]

show platform tcam table equal-cost-route [ asic number [ detail [ invalid ] ] | [ index number
[ detail [ invalid ] ] | invalid | num number [ detail [ invalid ] ] | invalid ] | [ invalid ] | [ num number
[ detail [ invalid ] ] | invalid ] ]

show platform tcam table local [ asic number [ detail [ invalid ] ] | [ index number [ detail [ invalid ] ]
| invalid | num number [ detail [ invalid ] ] | invalid ] | [ invalid ] | [ num number [ detail [ invalid ] ]
| invalid ] ]

show platform tcam table mac-address [ asic number [ detail [ invalid ] ] | [ index number [ detail
[ invalid ] ] | invalid | num number [ detail [ invalid ] ] | invalid ] | [ invalid ] | [ num number [ detail
[ invalid ] ] | invalid ] ]

show platform tcam table qos [ asic number [ detail [ invalid ] ] | [ index number [ detail [ invalid ] ] |
invalid | num number [ detail [ invalid ] ] | invalid ] | [ invalid ] | [ num number [ detail [ invalid ] ]
| invalid ] ]

show platform tcam table secondary [ asic number [ detail [ invalid ] ] | [ index number [ detail
[ invalid ] ] | invalid | num number [ detail [ invalid ] ] | invalid ] | [ invalid ] | [ num number [ detail
[ invalid ] ] | invalid ] ]

show platform tcam table station [ asic number [ detail [ invalid ] ] | [ index number [ detail
[ invalid ] ] | invalid | num number [ detail [ invalid ] ] | invalid ] | [ invalid ] | [ num number [ detail
[ invalid ] ] | invalid ] ]

show platform tcam table vlan-list [ [ asic number [ detail [ invalid ] ] | [ index number [ detail
[ invalid ] ] | invalid | num number [ detail [ invalid ] ] | invalid ] | [ invalid ] | [ num number [ detail
[ invalid ] ] | invalid ] ] ]

```

## Syntax Description

<b>handle</b> <i>number</i>	Display the TCAM handle. The range is 0 to 4294967295.
<b>log-results</b>	Display the TCAM log results.

<b>table</b> { <b>acl</b>   <b>all</b>   <b>equal-cost-route</b>   <b>ipv6</b> { <b>acl</b>   <b>qos</b>   <b>secondary</b> }   <b>local</b>   <b>mac-address</b>   <b>qos</b>   <b>secondary</b>   <b>station</b>   <b>vlan-list</b> }	Display lookup and forwarding table information. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>acl</b>—Display the access-control list (ACL) table.</li> <li>• <b>all</b>—Display all the TCAM tables.</li> <li>• <b>equal-cost-route</b>—Display the equal-cost-route table.</li> <li>• <b>local</b>—Display the local table.</li> <li>• <b>mac-address</b>—Display the MAC-address table.</li> <li>• <b>qos</b>—Display the QoS table.</li> <li>• <b>secondary</b>—Display the secondary table.</li> <li>• <b>station</b>—Display the station table.</li> <li>• <b>vlan-list</b>—Display the VLAN list table.</li> </ul>
<b>usage</b>	Display the CAM and forwarding table usage.
[[ <b>asic number</b> [ <b>detail</b> [ <b>invalid</b> ]]   [ <b>index number</b> [ <b>detail</b> [ <b>invalid</b> ]]   <b>invalid</b>   <b>num number</b> [ <b>detail</b> [ <b>invalid</b> ]]   <b>invalid</b> ]   [ <b>invalid</b> ]   [ <b>num number</b> [ <b>detail</b> [ <b>invalid</b> ]]   <b>invalid</b> ]]	Display information. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>asic number</b>—Display information for the specified ASIC device ID. The range is 0 to 15.</li> <li>• <b>detail</b> [<b>invalid</b>]—(Optional) Display valid or invalid details.</li> <li>• <b>index number</b>—(Optional) Display information for the specified TCAM table index. The range is 0 to 32768.</li> <li>• <b>num number</b>—(Optional) Display information for the specified TCAM table number. The range is 0 to 32768.</li> </ul>

**Note**

Though visible in the command-line help strings, the **ipv6**, **multicast-expansion** and **usage** keywords are not supported.

**Command Modes**

Privileged EXEC

**Command History**

Release	Modification
12.2(44)EY	This command was introduced.

**Usage Guidelines**

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

# show platform vlan

Use the **show platform vlan** privileged EXEC command to display platform-dependent VLAN information.

```
show platform vlan { mapping | misc | mvid | refcount | rpc { receive | transmit } }
```

## Syntax Description

<b>mapping</b>	See the <a href="#">show platform vlan mapping</a> command.
<b>misc</b>	Display miscellaneous VLAN module information.
<b>mvid</b>	Display the mapped VLAN ID (MVID) allocation information.
<b>refcount</b>	Display the VLAN lock module-wise reference counts.
<b>rpc { receive   transmit }</b>	Display remote procedure call (RPC) messages. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>receive</b>—Display received information.</li> <li>• <b>transmit</b>—Display sent information.</li> </ul>



## Note

Though visible in the command-line help strings, the **prune** keyword is not supported.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EY	This command was introduced.

## Usage Guidelines

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

# show platform vlan mapping

Use the **show platform vlan mapping** privileged EXEC command to display platform-dependent VLAN mapping information.

**show platform vlan mapping** [*interface-id* [*vlan-id*] | **handle** *handle-id* | **usage**]

Syntax Description		
<i>interface-id</i>	(Optional) Enter the physical interface ID or port channel number. Port channel range is form 1 to 48.	
<i>vlan-id</i>	(Optional) Display information for the original VLAN on the wire, the customer VLAN ID (C-VLAN). VLAN ID range is from 1 to 4094.	
<b>handle</b> <i>handle-id</i>	(Optional) Display the VLAN mapping handle details. The handle-ID range is from 0 to 65535.	
<b>usage</b>	(Optional) Display the VLAN mapping hardware resource usage.	

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EY	This command was introduced.

**Usage Guidelines** Use this command 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.

**Examples** These are examples of output from the show platform vlan mapping command:

```
Switch# show platform vlan mapping fastethernet 0/1
Platform Vlan Mapping Information
-----
Interface Fa0/1:
  1-to-1
  option:      0
  cvlan:      10
  cvlanlist:  10
  cinnervlan:  0
  spvlan:    100 (0)
  spinnervlan: 0
  ingress block: 100
  egress block: 10
  hw state: on-hold
  ingress handle: 0, egress handle: 1
  ingress block handle: 2, egress block handle: 3

Switch# show platform vlan mapping handle 1
Platform Vlan Mapping Information
-----
Handle number: 1 Type: 1-to-1
Asic: 0 Region: Match 1 vlan
```

■ **show platform vlan mapping**

```

First entry: 977 Number of entries: 1
Index  TCAM ENTRY          TCAM MASK          DESCRIPTOR
=====
977    7C006400 00000000      FE0FFF00 00004000      8010100A 00000000
Stat handle: 1 Packets: 0, Bytes: 0

```

Switch# **show platform vlan mapping usage**

Platform Vlan Mapping Information

-----

Port ASIC 0

Region Name	Min	Start	End	Used	Avail	Total	Percentage
Loopback	* 0	0	6	0	6	6	0%
Drop	0	6	492	0	486	486	0%
Match 2 vlans	0	492	976	0	484	484	0%
Match 1 vlan	0	976	1460	2	482	484	0%
Default operations	104	1460	1564	0	104	104	0%
Vlan blocking	0	1564	2048	2	482	484	0%

-----

\* = region needs compacting

Section Total

Start	End	Used	Avail	Total	Percentage
0	2048	4	2044	2048	0%





## APPENDIX **D**

# Acknowledgments for Open-Source Software

---

The Cisco IOS software pipe command uses Henry Spencer's regular expression library (regex). The most recent version of the library has been modified slightly in the Catalyst operating system software to maintain compatibility with earlier versions of the library.

Henry Spencer's regular expression library (regex). Copyright 1992, 1993, 1994, 1997 Henry Spencer. All rights reserved. This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from flaws in it.
2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation.
3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation.
4. This notice may not be removed or altered.





## INDEX

---

### A

aaa accounting dot1x command [2-1](#)  
aaa authentication dot1x command [2-3](#)  
AAA methods [2-3](#)  
access control entries  
    See ACEs  
access control lists  
    See ACLs  
access groups  
    IP [2-151](#)  
    MAC, displaying [2-536](#)  
    matching for QoS classification [2-287](#)  
access list, IPv6 [2-220](#)  
access mode [2-690](#)  
access ports [2-690](#)  
ACEs [2-91](#), [2-332](#)  
ACLs  
    as match criteria for QoS classes [2-287](#)  
    deny [2-89](#)  
    displaying [2-412](#)  
    for non-IP protocols [2-265](#)  
    IP [2-151](#)  
    on Layer 2 interfaces [2-151](#)  
    permit [2-330](#)  
action command [2-5](#)  
address aliasing [2-310](#)  
aggregate policers  
    applying [2-343](#)  
    creating [2-338](#)  
    displaying [2-568](#)  
    QoS [2-340](#)  
aggregate-port learner [2-319](#)

alarm-contact command [2-7](#)  
alarm-contact status, displaying [2-445](#)  
allowed VLANs [2-706](#)  
archive download-sw command [2-9](#)  
archive tar command [2-12](#)  
archive upload-sw command [2-15](#)  
arp (boot loader) command [A-2](#)  
arp access-list command [2-17](#)  
attaching policy maps to interfaces [2-393](#)  
authorization state of controlled port [2-105](#)  
autonegotiation of duplex mode [2-117](#)

---

### B

backup interfaces  
    configuring [2-683](#)  
    displaying [2-467](#)  
bandwidth, configuring for QoS [2-19](#)  
bandwidth command [2-19](#)  
boot (boot loader) command [A-3](#)  
boot config-file command [2-23](#)  
boot enable-break command [2-24](#)  
boot helper command [2-25](#)  
boot helper-config file command [2-26](#)  
booting  
    Cisco IOS image [2-29](#)  
    displaying environment variables [2-417](#)  
    interrupting [2-24](#)  
    manually [2-27](#)

## boot loader

- accessing [A-1](#)

## booting

- Cisco IOS image [A-3](#)

- helper image [2-25](#)

## directories

- creating [A-18](#)

- displaying a list of [A-8](#)

- removing [A-22](#)

## displaying

- available commands [A-13](#)

- memory heap utilization [A-14](#)

- version [A-29](#)

## environment variables

- described [A-23](#)

- displaying settings [A-23](#)

- location of [A-24](#)

- setting [A-23](#)

- unsetting [A-27](#)

## files

- copying [A-6](#)

- deleting [A-7](#)

- displaying a list of [A-8](#)

- displaying the contents of [A-5, A-19, A-26](#)

- renaming [A-20](#)

## file system

- formatting [A-11](#)

- initializing flash [A-10](#)

- running a consistency check [A-12](#)

prompt [A-1](#)

- resetting the system [A-21](#)

boot manual command [2-27](#)boot private-config-file command [2-28](#)boot system command [2-29](#)BPDU filtering, for spanning tree [2-628, 2-666](#)BPDU guard, for spanning tree [2-630, 2-666](#)broadcast storm control [2-676](#)bundling characteristics, UNI [2-127](#)burst bytes, in QoS policers [2-334, 2-339](#)**C**cat (boot loader) command [A-5](#)CBWFQ, configuring [2-19](#)CDP, enabling protocol tunneling for [2-245](#)CFM [2-318](#)CFM as OAM protocol [2-318](#)channel-group command [2-30](#)channel-protocol command [2-34](#)child policy maps [2-395](#)class-based traffic shaping [2-410](#)

class-based weighted fair queuing

- See CBWFQ

class command [2-36](#)class-map command [2-38](#)class-map configuration mode [2-38](#)

## class maps

- creating [2-38](#)

- defining the match criteria [2-288, 2-290](#)

- displaying [2-421](#)

- matching in [2-38](#)

## class of service

- See CoS

clear ip arp inspection log command [2-40](#)clear ip arp inspection statistics command [2-41](#)clear ipc command [2-44](#)clear ipv6 dhcp conflict command [2-45](#)clear l2protocol-tunnel counters command [2-46](#)clear lacp command [2-47](#)clear logging onboard command [2-48](#)clear mac address-table command [2-49, 2-50](#)clear pagp command [2-51, 2-55](#)clear policer cpu uni-eni counters command [2-52](#)clear port-security command [2-53](#)clear spanning-tree counters command [2-56](#)clear spanning-tree detected-protocols command [2-57](#)clear vmps statistics command [2-59](#)command modes defined [1-1](#)committed information rate in QoS policers [2-334, 2-338](#)

- configuration files
    - password recovery disable considerations [A-1](#)
    - specifying the name [2-23, 2-28](#)
  - configuring multiple interfaces [2-147](#)
  - conform-action command [2-60](#)
  - control-plane policer [2-52](#)
  - control-plane policer information, displaying [2-569](#)
  - control-plane security [2-345](#)
  - control plane statistics, clearing [2-52](#)
  - copy (boot loader) command [A-6](#)
  - copy logging onboard module command [2-62](#)
  - CoS
    - as match criteria for QoS groups [2-288](#)
    - for QoS classification [2-397](#)
    - setting value in policy maps [2-397](#)
  - CoS value, assigning to Layer 2 protocol packets [2-248](#)
  - CPU ASIC statistics, displaying [2-422](#)
  - CPU protection policers, displaying [C-24](#)
  - cpu traffic qos cos command [2-64](#)
  - cpu traffic qos dscp command [2-68](#)
  - cpu traffic qos precedence command [2-73](#)
  - cpu traffic qos qos-group command [2-76](#)
- 
- D**
- DC power supply [2-354](#)
  - debug backup command [B-2](#)
  - debug dot1x command [B-3](#)
  - debug etherchannel command [B-4](#)
  - debug interface command [B-7](#)
  - debug ip dhcp snooping command [B-8](#)
  - debug ip igmp filter command [B-9](#)
  - debug ip igmp max-groups command [B-10](#)
  - debug ip igmp snooping command [B-11](#)
  - debug ip sla error twamp connection command [B-12](#)
  - debug ip sla error twamp control reflector command [B-14](#)
  - debug ip sla error twamp control server command [B-16](#)
  - debug ip sla error twamp session command [B-18](#)
  - debug ip sla trace twamp connection command [B-20](#)
  - debug ip sla trace twamp control reflector command [B-22](#)
  - debug ip sla trace twamp control server command [B-24](#)
  - debug ip sla trace twamp session command [B-26](#)
  - debug ip verify source packet command [B-28](#)
  - debug lacp command [B-29](#)
  - debug mac-notification command [B-30](#)
  - debug matm command [B-31](#)
  - debug matm move update command [B-32](#)
  - debug monitor command [B-33](#)
  - debug mvrdbg command [B-34](#)
  - debug nvram command [B-35](#)
  - debug pagp command [B-36](#)
  - debug platform acl command [B-37](#)
  - debug platform backup interface command [B-38](#)
  - debug platform cfm command [B-39](#)
  - debug platform cpu-queues command [B-40](#)
  - debug platform dot1ad command [B-42](#)
  - debug platform dot1x command [B-43](#)
  - debug platform etherchannel command [B-44](#)
  - debug platform forw-tcam command [B-45](#)
  - debug platform ip arp inspection command [B-46](#)
  - debug platform ipc command [B-55](#)
  - debug platform ip dhcp command [B-47](#)
  - debug platform ip igmp snooping command [B-48](#)
  - debug platform ip multicast command [B-50](#)
  - debug platform ip source-guard command [B-52](#)
  - debug platform led command [B-56](#)
  - debug platform matm command [B-57](#)
  - debug platform messaging application command [B-58](#)
  - debug platform phy command [B-59](#)
  - debug platform pm command [B-61](#)
  - debug platform policer cpu uni-eni command [B-63](#)
  - debug platform port-asic command [B-64](#)
  - debug platform port-security command [B-65](#)
  - debug platform qos-acl-tcam command [B-66](#)
  - debug platform qos-manager command [B-67](#)
  - debug platform remote-commands command [B-68](#)
  - debug platform rep command [B-69](#)
  - debug platform resource-manager command [B-70](#)

- debug platform snmp command [B-71](#)
- debug platform span command [B-72](#)
- debug platform supervisor-asic command [B-73](#)
- debug platform sw-bridge command [B-74](#)
- debug platform team command [B-75](#)
- debug platform uddl command [B-77](#)
- debug platform vlan command [B-78](#)
- debug pm command [B-79](#)
- debug port-security command [B-81](#)
- debug qos-manager command [B-83](#)
- debug rep command [B-82](#)
- debug spanning-tree bpdu command [B-86](#)
- debug spanning-tree bpdu-opt command [B-87](#)
- debug spanning-tree command [B-84](#)
- debug spanning-tree mstp command [B-88](#)
- debug spanning-tree switch command [B-90](#)
- debug sw-vlan command [B-92](#)
- debug sw-vlan ifs command [B-93](#)
- debug sw-vlan notification command [B-94](#)
- debug uddl command [B-96](#)
- debug vqpc command [B-98](#)
- default policer configuration
  - NNIs [C-26](#)
  - UNIs [C-25](#)
- define interface-range command [2-78](#)
- delete (boot loader) command [A-7](#)
- delete command [2-80](#)
- deny (ARP access-list configuration) command [2-81](#)
- deny (IPv6) command [2-83](#)
- deny command [2-89](#)
- detect mechanism, causes [2-118](#)
- DHCP snooping
  - accepting untrusted packets from edge switch [2-176](#)
  - enabling
    - on a VLAN [2-182](#)
    - option 82 [2-174, 2-176](#)
    - trust on an interface [2-180](#)
  - error recovery timer [2-120](#)
  - rate limiting [2-179](#)
- DHCP snooping binding database
  - binding file, configuring [2-172](#)
  - bindings
    - adding [2-170](#)
    - deleting [2-170](#)
    - displaying [2-488](#)
  - clearing database agent statistics [2-42](#)
  - database agent, configuring [2-172](#)
  - displaying
    - binding entries [2-488](#)
    - database agent status [2-490, 2-492](#)
    - renewing [2-369](#)
- diagnostic monitor command [2-92](#)
- diagnostic schedule test command [2-94](#)
- diagnostic start test command [2-96](#)
- differentiated service code point
  - See DSCP
- Digital Optical Monitoring
  - see DoM
- dir (boot loader) command [A-8](#)
- directories, deleting [2-80](#)
- DoM
  - displaying supported transceivers [2-479, 2-618, 2-619](#)
- domains, CFM [2-318](#)
- dot1x default command [2-98](#)
- dot1x host-mode command [2-99](#)
- dot1x initialize command [2-101](#)
- dot1x max-req command [2-102, 2-104](#)
- dot1x port-control command [2-105](#)
- dot1x re-authenticate command [2-107](#)
- dot1x reauthentication command [2-108](#)
- dot1x supplicant force-multicast command [2-109](#)
- dot1x system-auth-control command [2-110](#)
- dot1x test eapol-capable command [2-111](#)
- dot1x test timeout command [2-112](#)
- dot1x timeout command [2-113](#)
- dot1x violation-mode command [2-115](#)
- drop eligibility indicator [2-399](#)
- drop eligibility indicator bit [2-290](#)

- dropping packets, with ACL matches [2-5](#)
- drop threshold, Layer 2 protocol tunneling [2-245](#)
- DSCP
  - as match criteria for QoS groups [2-292, 2-298](#)
  - for QoS traffic marking [2-401](#)
  - setting in policy maps [2-401](#)
- dual IPv4 and IPv6 templates [2-325](#)
- dual-purpose uplink ports, selecting the type [2-303](#)
- duplex command [2-116](#)
- dynamic-access ports
  - configuring [2-681](#)
  - restrictions [2-682](#)
- dynamic ARP inspection
  - ARP ACLs
    - apply to a VLAN [2-156](#)
    - define [2-17](#)
    - deny packets [2-81](#)
    - display [2-416](#)
    - permit packets [2-323](#)
  - clear
    - log buffer [2-40](#)
    - statistics [2-41](#)
  - display
    - ARP ACLs [2-416](#)
    - configuration and operating state [2-483](#)
    - log buffer [2-483](#)
    - statistics [2-483](#)
    - trust state and rate limit [2-483](#)
  - enable per VLAN [2-165](#)
  - error detection for [2-118](#)
  - error recovery timer [2-120](#)
  - log buffer
    - clear [2-40](#)
    - configure [2-160](#)
    - display [2-483](#)
  - rate-limit incoming ARP packets [2-158](#)
  - statistics
    - clear [2-41](#)
    - display [2-483](#)

- trusted interface state [2-162](#)
- type of packet logged [2-166](#)
- validation checks [2-163](#)

Dynamic Host Configuration Protocol (DHCP)  
See DHCP snooping

---

## E

- EAP-request/identity frame
  - maximum number to send [2-104](#)
  - response time before retransmitting [2-113](#)
- E-LMI
  - enabling [2-125](#)
  - mapping [2-127](#)
- environment variables, displaying [2-417](#)
- errdisable detect cause command [2-118](#)
- errdisable recovery command [2-120](#)
- error conditions, displaying [2-449](#)
- error disable detection [2-118](#)
- error-disabled interfaces, displaying [2-467](#)
- EtherChannel
  - assigning Ethernet interface to channel group [2-30](#)
  - creating port-channel logical interface [2-145](#)
  - debug EtherChannel/PAgP, display [B-4](#)
  - debug platform-specific events, display [B-44](#)
  - displaying [2-453](#)
  - enabling Layer 2 protocol tunneling for
    - LACP [2-246](#)
    - PAgP [2-246](#)
    - UDLD [2-246](#)
  - interface information, displaying [2-467](#)
  - LACP
    - clearing channel-group information [2-47](#)
    - debug messages, display [B-29](#)
    - displaying [2-523](#)
    - modes [2-30](#)
    - port priority for hot-standby ports [2-249](#)
    - restricting a protocol [2-34](#)
    - system priority [2-251](#)

load-distribution methods [2-350](#)

PAgP

- aggregate-port learner [2-319](#)
- clearing channel-group information [2-51](#)
- debug messages, display [B-36](#)
- displaying [2-564](#)
- error detection for [2-118](#)
- error recovery timer [2-120](#)
- learn method [2-319](#)
- modes [2-30](#)
- physical-port learner [2-319](#)
- priority of interface for transmitted traffic [2-321](#)

Ethernet controller, internal register display [2-424](#)

ethernet dot1ad command [2-122](#)

ethernet evc command [2-124](#)

ethernet lmi ce-vlan map command [2-125, 2-127](#)

ethernet lmi command [2-125](#)

ethernet lmi global command [2-125](#)

Ethernet Local Management Interface

- See E-LMI

ethernet loopback interface configuration command [2-129](#)

ethernet loopback privileged EXEC command [2-132](#)

ethernet oam remote-failure command [2-134](#)

Ethernet service

- debugging [B-5](#)
- displaying [2-458](#)

Ethernet service instance [2-389](#)

Ethernet service interfaces [2-461](#)

Ethernet statistics, collecting [2-385](#)

Ethernet UNI configuration [2-136](#)

ethernet uni id command [2-138](#)

Ethernet virtual connections

- See EVCs

EVC configuration mode [2-124](#)

EVCs [2-124](#)

- and VLANs [2-136](#)
- service instances [2-389](#)
- UNI counts [2-729](#)

EVC service

- point-to-multipoint [2-729](#)
- point-to-point [2-729](#)

exceed-action command [2-139](#)

extended-range VLANs

- and allowed VLAN list [2-706](#)
- configuring [2-735](#)

extended system ID for STP [2-636](#)

external alarms, configuring [2-7](#)

---

## F

failure logging data

- clearing [2-48](#)
- copying [2-62](#)

fan information, displaying [2-445](#)

files, deleting [2-80](#)

flash\_init (boot loader) command [A-10](#)

Flex Links

- configuring [2-683](#)
- configuring preferred VLAN [2-685](#)
- displaying [2-467](#)

flowcontrol command [2-141](#)

format (boot loader) command [A-11](#)

forwarding packets, with ACL matches [2-5](#)

forwarding results, display [C-8](#)

frame forwarding information, displaying [C-8](#)

front-end controller counter and status information [C-10](#)

fsck (boot loader) command [A-12](#)

---

## G

global configuration mode [1-2, 1-3](#)

---

## H

hardware ACL statistics [2-412](#)

health-monitoring diagnostic testing [2-92](#)



help (boot loader) command [A-13](#)  
 host connection, port configuration [2-689](#)  
 host ports, private VLANs [2-693](#)  
 hw-module module logging onboard command [2-143](#)

## I

IEEE 802.1ag Connectivity Fault Management

See CFM

IEEE 802.1Q trunk ports and native VLANs [2-740](#)

IEEE 802.1Q tunnel ports

configuring [2-690](#)

displaying [2-441](#)

limitations [2-691](#)

IEEE 802.1x

and switchport modes [2-691](#)

violation error recovery [2-120](#)

See also port-based authentication

IGMP filters

applying [2-185](#)

debug messages, display [B-9](#)

IGMP groups, setting maximum [2-187](#)

IGMP maximum groups, debugging [B-10](#)

IGMP profiles

creating [2-189](#)

displaying [2-497](#)

IGMP snooping

adding ports as a static member of a group [2-204](#)

displaying [2-498, 2-502, 2-503](#)

enabling [2-191](#)

enabling the configurable-leave timer [2-193](#)

enabling the Immediate-Leave feature [2-201](#)

flooding query count [2-199](#)

interface topology change notification behavior [2-200](#)

multicast table [2-500](#)

querier [2-195](#)

query solicitation [2-199](#)

report suppression [2-197](#)

switch topology change notification behavior [2-199](#)

images

See software images

Immediate-Leave feature, MVR [2-312](#)

immediate-leave processing [2-201](#)

Immediate-Leave processing, IPv6 [2-241](#)

input policy maps

and ACL classification [2-287](#)

and aggregate policers [2-340](#)

commands not supported in [2-348](#)

configuration guidelines [2-348](#)

interface command [2-149](#)

interface configuration mode [1-2, 1-4](#)

interface port-channel command [2-145](#)

interface range command [2-147](#)

interface-range macros [2-78](#)

interfaces

assigning Ethernet interface to channel group [2-30](#)

configuring [2-116](#)

configuring multiple [2-147](#)

creating port-channel logical [2-145](#)

debug messages, display [B-7](#)

disabling [2-613](#)

displaying the MAC address table [2-546](#)

restarting [2-613](#)

interface speed, configuring [2-674](#)

internal registers, displaying [2-424, 2-431](#)

Internet Group Management Protocol

See IGMP

invalid GBIC

error detection for [2-118](#)

error recovery timer [2-120](#)

ip address command [2-154](#)

IP addresses, setting [2-154](#)

IP address matching [2-285](#)

ip arp inspection filter vlan command [2-156](#)

ip arp inspection limit command [2-158](#)

ip arp inspection log-buffer command [2-160](#)

ip arp inspection trust command [2-162](#)

ip arp inspection validate command [2-163](#)

- ip arp inspection vlan command [2-165](#)
- ip arp inspection vlan logging command [2-166](#)
- IP DHCP snooping
  - See DHCP snooping
- ip dhcp snooping binding command [2-170](#)
- ip dhcp snooping command [2-169](#)
- ip dhcp snooping database command [2-172](#)
- ip dhcp snooping information option allow-untrusted command [2-176](#)
- ip dhcp snooping information option command [2-174](#)
- ip dhcp snooping information option format remote-id command [2-178](#)
- ip dhcp snooping limit rate command [2-179](#)
- ip dhcp snooping trust command [2-180](#)
- ip dhcp snooping verify command [2-181](#)
- ip dhcp snooping vlan command [2-182](#)
- ip dhcp snooping vlan information option format-type circuit-id string command [2-183](#)
- ip igmp filter command [2-185](#)
- ip igmp max-groups command [2-187](#), [2-214](#), [2-216](#)
- ip igmp profile command [2-189](#)
- ip igmp snooping command [2-191](#)
- ip igmp snooping last-member-query-interval command [2-193](#)
- ip igmp snooping querier command [2-195](#)
- ip igmp snooping report-suppression command [2-197](#)
- ip igmp snooping tcn command [2-199](#)
- ip igmp snooping tcn flood command [2-200](#)
- ip igmp snooping vlan immediate-leave command [2-201](#)
- ip igmp snooping vlan mrouter command [2-202](#)
- ip igmp snooping vlan static command [2-204](#)
- IP multicast addresses [2-309](#)
- IP precedence, as match criteria for QoS groups [2-294](#)
- ip sla responder twamp command [2-206](#)
- ip sla server twamp command [2-208](#)
- ip source binding command [2-210](#)
- IP source guard
  - disabling [2-218](#)
  - displaying
    - binding entries [2-509](#)
    - configuration [2-510](#)
  - enabling [2-218](#)
  - static IP source bindings [2-210](#)
- IP source guard, displaying dynamic binding entries [2-488](#)
- ip ssh command [2-212](#)
- IPv6 access list, deny conditions [2-83](#)
- ipv6 access-list command [2-220](#)
- ipv6 address dhcp command [2-222](#)
- ipv6 dhcp client request vendor command [2-223](#)
- ipv6 dhcp ping packets command [2-224](#)
- ipv6 dhcp pool command [2-225](#)
- ipv6 dhcp server command [2-228](#)
- ipv6 mld snooping command [2-230](#)
- ipv6 mld snooping last-listener-query count command [2-232](#)
- ipv6 mld snooping last-listener-query-interval command [2-234](#)
- ipv6 mld snooping listener-message-suppression command [2-236](#)
- ipv6 mld snooping robustness-variable command [2-237](#)
- ipv6 mld snooping tcn command [2-239](#)
- ipv6 mld snooping vlan command [2-241](#)
- IPv6 SDM template [2-386](#)
- ipv6 traffic-filter command [2-243](#)
- ip verify source command [2-218](#)

---

## J

- jumbo frames
  - See MTU

---

## L

- l2protocol-tunnel command [2-245](#)
- l2protocol-tunnel cos command [2-248](#)

- LACP
  - See EtherChannel
- lacp port-priority command [2-249](#)
- lacp system-priority command [2-251](#)
- Layer 2 mode, enabling [2-679](#)
- Layer 2 protocol ports, displaying [2-521](#)
- Layer 2 protocol-tunnel
  - error detection for [2-118](#)
  - error recovery timer [2-120](#)
- Layer 2 protocol tunnel counters [2-46](#)
- Layer 2 protocol tunneling error recovery [2-247](#)
- Layer 2 traceroute
  - IP addresses [2-722](#)
  - MAC addresses [2-719](#)
- Layer 3 mode, enabling [2-679](#)
- line configuration mode [1-2, 1-4](#)
- Link Aggregation Control Protocol
  - See EtherChannel
- link flap
  - error detection for [2-118](#)
  - error recovery timer [2-120](#)
- link state group command [2-253](#)
- link state track command [2-255](#)
- load-distribution methods for EtherChannel [2-350](#)
- location (global configuration) command [2-256](#)
- location (interface configuration) command [2-258](#)
- logging event command [2-260](#)
- logging file command [2-261](#)
- logical interface [2-145](#)
- loopback error
  - detection for [2-118](#)
  - recovery timer [2-120](#)
- loop guard, for spanning tree [2-638, 2-642](#)
- mac access-list extended command [2-265](#)
- MAC access lists [2-89](#)
- MAC addresses
  - disabling MAC address learning per VLAN [2-268](#)
  - displaying
    - aging time [2-540](#)
    - all [2-539](#)
    - dynamic [2-544](#)
    - MAC address-table move updates [2-549](#)
    - notification settings [2-548, 2-550](#)
    - number of addresses in a VLAN [2-542](#)
    - per interface [2-546](#)
    - per VLAN [2-554](#)
    - static [2-552](#)
    - static and dynamic entries [2-537](#)
  - dynamic
    - aging time [2-267](#)
    - deleting [2-49](#)
    - displaying [2-544](#)
  - enabling MAC address notification [2-272](#)
  - enabling MAC address-table move update [2-270](#)
  - matching [2-285](#)
  - static
    - adding and removing [2-274](#)
    - displaying [2-552](#)
    - dropping on an interface [2-275](#)
  - tables [2-539](#)
- MAC address notification, debugging [B-30](#)
- mac address-table aging-time [2-263, 2-285](#)
- mac address-table aging-time command [2-267](#)
- mac address-table learning command [2-268](#)
- mac address-table move update command [2-270](#)
- mac address-table notification command [2-272](#)
- mac address-table static command [2-274](#)
- mac address-table static drop command [2-275](#)
- macro description command [2-279](#)
- macro global command [2-280](#)
- macro global description command [2-282](#)
- macro name command [2-283](#)

---

## M

- mac access-group command [2-263](#)
- MAC access-groups, displaying [2-536](#)
- MAC access list configuration mode [2-265](#)

## macros

- adding a description [2-279](#)
- adding a global description [2-282](#)
- applying [2-280](#)
- creating [2-283](#)
- displaying [2-566](#)
- interface range [2-78, 2-147](#)
- specifying parameter values [2-280](#)
- tracing [2-280](#)

maintenance end points [2-729](#)

mapping tables, QoS [2-715](#)

## maps

## class

- creating [2-38](#)

## VLAN

- creating [2-738](#)
- defining [2-285](#)
- displaying [2-607](#)

match access-group command [2-287](#)

match cos command [2-288](#)

match dot1ad dei command [2-290](#)

match ip dscp command [2-292](#)

match ip precedence command [2-294](#)

match qos-group command [2-296](#)

match vlan command [2-298](#)

maximum transmission unit

See MTU

mdix auto command [2-301](#)

ME 3400EG-2CS switch policers [C-24](#)

ME 3400E-24TS switch policers [C-24](#)

ME 3400EG-12CS switch policers [C-24](#)

media-type command [2-303](#)

memory (boot loader) command [A-14](#)

mgmt\_clr (boot loader) command [A-15](#)

mgmt\_init (boot loader) command [A-16, A-17](#)

mkdir (boot loader) command [A-18](#)

## MLD snooping

- configuring [2-236, 2-237](#)
- configuring queries [2-232, 2-234](#)
- configuring topology change notification [2-239](#)
- enabling [2-230](#)

MLD snooping on a VLAN, enabling [2-241](#)

mode, MVR [2-309](#)

modes, commands [1-1](#)

monitor session command [2-305](#)

more (boot loader) command [A-19](#)

## MSTP

displaying [2-588](#)

interoperability [2-57](#)

link type [2-640](#)

## MST region

- aborting changes [2-646](#)
- applying changes [2-646](#)
- configuration name [2-646](#)
- configuration revision number [2-647](#)
- current or pending display [2-647](#)
- displaying [2-588](#)
- MST configuration mode [2-646](#)
- VLANs-to-instance mapping [2-646](#)

path cost [2-648](#)

protocol mode [2-644](#)

restart protocol migration process [2-57](#)

## root port

- loop guard [2-638](#)
- preventing from becoming designated [2-638](#)
- restricting which can be root [2-638](#)
- root guard [2-638](#)

## root switch

- affects of extended system ID [2-636](#)
- hello-time [2-651, 2-662](#)
- interval between BDPU messages [2-653](#)
- interval between hello BPDU messages [2-651, 2-662](#)
- max-age [2-653](#)

- maximum hop count before discarding BPDUs [2-655](#)
  - port priority for selection of [2-657](#)
  - primary or secondary [2-662](#)
  - switch priority [2-660](#)
- state changes
  - blocking to forwarding state [2-669](#)
  - enabling BPDU filtering [2-628, 2-666](#)
  - enabling BPDU guard [2-630, 2-666](#)
  - enabling Port Fast [2-666, 2-669](#)
  - forward-delay time [2-650](#)
  - length of listening and learning states [2-650](#)
  - rapid transition to forwarding [2-640](#)
  - shutting down Port Fast-enabled ports [2-666](#)
- state information display [2-587](#)

MTU

- configuring size [2-712](#)
- displaying global setting [2-595](#)

multicast group address, MVR [2-312](#)

multicast groups, MVR [2-310](#)

Multicast Listener Discovery

- See MLD

multicast router learning method [2-202](#)

multicast router ports, configuring [2-202](#)

multicast router ports, IPv6 [2-241](#)

multicast storm control [2-676](#)

multicast VLAN, MVR [2-310](#)

multicast VLAN registration

- See MVR

multiple hosts on authorized port [2-99](#)

Multiple Spanning Tree Protocol

- See MSTP

multiplexing, UNI [2-136](#)

MVR

- and address aliasing [2-310](#)
- configuring [2-309](#)
- configuring interfaces [2-312](#)
- debug messages, display [B-34](#)
- displaying [2-558](#)

- displaying interface information [2-560](#)
  - members, displaying [2-562](#)
- mvr (global configuration) command [2-309](#)
- mvr (interface configuration) command [2-312](#)
- mvr vlan group command [2-313](#)

---

## N

- native VLANs [2-706](#)
- native VLAN tagging [2-740](#)
- network node interface [2-352](#)
- no authentication logging verbose [2-315](#)
- no dot1x logging verbose [2-316](#)
- no mab logging verbose [2-317](#)
- nonegotiate, speed [2-674, 2-675](#)
- non-IP protocols
  - denying [2-89](#)
  - forwarding [2-330](#)
- non-IP traffic access lists [2-265](#)
- non-IP traffic forwarding
  - denying [2-89](#)
  - permitting [2-330](#)
- normal-range VLANs [2-735](#)
- no vlan command [2-735](#)

---

## O

- OAM PDUs [2-134](#)
- OAM protocol [2-318](#)
- oam protocol cfm svlan command [2-318](#)
- on-board failure logging, displaying [2-532](#)
- on-board failure logging, enabling [2-143](#)

- online diagnostics
    - enabling
      - scheduling [2-94](#)
    - global configuration mode
      - clearing test-based testing schedule [2-94](#)
      - setting test-based testing [2-94](#)
      - setting up test-based testing [2-94](#)
    - removing scheduling [2-94](#)
    - scheduled switchover
      - disabling [2-94](#)
      - enabling [2-94](#)
    - setting test interval [2-94](#)
    - starting testing [2-96](#)
  - online diagnostic tests, displaying results [2-437](#)
  - online diagnostic tests, starting [2-96](#)
  - operation, administration, and maintenance protocol
    - See OAM
  - output policy maps
    - and QoS group classification [2-296](#)
    - and traffic shaping [2-410](#)
    - commands not supported in [2-348](#)
    - configuration guidelines [2-348](#)
    - priority in [2-357](#)
    - queue limit in [2-364](#)
- 
- P**
- PAGP
    - See EtherChannel
  - pagp learn-method command [2-319](#)
  - pagp port-priority command [2-321](#)
  - parent policy maps [2-395](#)
  - password-recovery mechanism, enabling and disabling [2-391](#)
  - permit (ARP access-list configuration) command [2-323](#)
  - permit (IPv6) command [2-325](#)
  - permit command [2-330](#)
  - per-VLAN spanning-tree plus
    - See STP
  - physical-port learner [2-319](#)
  - PID, displaying [2-482](#)
  - PIM-DVMRP, as multicast router learning method [2-202](#)
  - police
    - multiple conform actions for a class [2-60](#)
    - multiple exceed actions for a class [2-139](#)
    - multiple violate actions for a class [2-733](#)
    - with priority [2-333](#)
  - police aggregate command [2-343](#)
  - police command [2-333](#)
  - policer aggregate command [2-338](#)
  - policer configuration
    - default for NNIs [C-26](#)
    - default for UNIs [C-25](#)
  - policer cpu uni command [2-345](#)
  - policers
    - aggregate [2-338, 2-343](#)
    - for CPU protection [2-345](#)
    - individual [2-333](#)
  - policy-map class, configuring multiple actions [2-60, 2-139, 2-733](#)
  - policy-map class configuration mode [2-36](#)
  - policy-map class police configuration mode [2-60, 2-336](#)
  - policy-map command [2-347](#)
  - policy-map configuration mode [2-347](#)
  - policy maps
    - and CoS classification [2-288](#)
    - and DSCP classification [2-292](#)
    - and IP precedence classification [2-294](#)
    - and policing [2-336](#)
    - applying [2-393](#)
    - applying to an interface [2-348, 2-393, 2-407](#)
    - child [2-395](#)
    - creating [2-347](#)
    - displaying [2-572](#)
    - hierarchical [2-395](#)
    - parent [2-395](#)



**Q**

## QoS

## aggregate policers

applying [2-343](#)creating [2-338](#)displaying [2-568](#)

## class maps

creating [2-38](#)defining the match criteria [2-288, 2-290](#)displaying [2-421](#)conform actions, configuring [2-61](#)displaying statistics for [2-572, C-33](#)exceed actions, configuring [2-140](#)

## policy maps

applying an aggregate policer [2-338, 2-343, 2-345, 2-395](#)applying to an interface [2-393, 2-407](#)creating [2-347](#)defining policers [2-333](#)displaying policy maps [2-572](#)setting CoS values [2-397](#)setting DSCP values [2-399, 2-401](#)setting IP precedence values [2-403](#)setting QoS group identifier [2-405](#)traffic classifications [2-36](#)

## table maps

configuring [2-715](#)displaying [2-596](#)violate actions, configuring [2-734](#)

## QoS groups

as match criteria [2-296](#)for QoS traffic classification [2-405](#)setting in policy maps [2-405](#)

## QoS match criteria

ACLs [2-287](#)CoS value [2-288](#)DSCP value [2-292, 2-298](#)precedence value [2-294](#)QoS group number [2-296](#)

quality of service

See QoS

querytime, MVR [2-309](#)queue-limit command [2-364](#)**R**

rapid per-VLAN spanning-tree plus

See STP

rapid PVST+

See STP

re-authenticating 802.1x-enabled ports [2-107](#)

re-authentication

periodic [2-108](#)time between attempts [2-113](#)receiver ports, MVR [2-312](#)receiving flow-control packets [2-141](#)

recovery mechanism

causes [2-120](#)display [2-419, 2-447, 2-451](#)timer interval [2-121](#)remote-span command [2-367](#)

Remote Switched Port Analyzer

See RSPAN

rename (boot loader) command [A-20](#)renew ip dhcp snooping database command [2-369](#)rep admin vlan command [2-370](#)rep block port command [2-371](#)rep lsl-age-timer command [2-375](#)rep preempt delay command [2-377](#)rep preempt segment command [2-379](#)rep segment command [2-380](#)rep stcn command [2-383](#)reset (boot loader) command [A-21](#)resource templates, displaying [2-585](#)rmdir (boot loader) command [A-22](#)rmon collection stats command [2-385](#)root guard, for spanning tree [2-638](#)



## routed ports

- IP addresses on [2-155](#)
- number supported [2-155](#)

## RSPAN

- configuring [2-305](#)
- displaying [2-556](#)
- filter RSPAN traffic [2-305](#)
- remote-span command [2-367](#)
- sessions
  - add interfaces to [2-305](#)
  - displaying [2-556](#)
  - start new [2-305](#)

---

**S**

## scheduled switchover

- disabling [2-94](#)
- enabling [2-94](#)

scheduling diagnostic tests [2-94](#)sdm prefer command [2-386](#)

## SDM templates

- allowed resources [2-387](#)
- displaying [2-585](#)
- dual IPv4 and IPv6 [2-386](#)

secure ports, limitations [2-698](#)sending flow-control packets [2-141](#)service instance command [2-389](#)service instances, displaying [2-459](#)service password-recovery command [2-391](#)service policy (policy-map class configuration) command [2-395](#)service-policy interface configuration command [2-393](#)service-policy policy-map class configuration command [2-395](#)set (boot loader) command [A-23](#)set cos command [2-397](#)set dot1ad dei command [2-399](#)set dscp command [2-401](#)set precedence command [2-403](#)set qos-group command [2-405](#)setup command [2-407](#)SFPs, displaying information about [2-482](#)shape average command [2-410](#)show access-lists command [2-412](#)show aggregate-policer command [2-595](#)show archive status command [2-415](#)show arp access-list command [2-416](#)show boot command [2-417](#)show class-map command [2-421](#)show controllers cpu-interface command [2-422](#)show controllers ethernet-controller command [2-424](#)show controllers tcam command [2-431](#)show controllers utilization command [2-433](#)show controller utilization command [2-433](#)show cpu traffic qos command [2-435](#)show diagnostic command [2-437](#)show dot1q-tunnel command [2-441](#)show dot1x command [2-442](#)show env command [2-445](#)show errdisable detect command [2-447](#)show errdisable flap-values command [2-449](#)show errdisable recovery command [2-451](#)show etherchannel command [2-453](#)show ethernet loopback command [2-456](#)show ethernet service evc command [2-458](#)show ethernet service instance command [2-459](#)show ethernet service interface command [2-461](#)show flowcontrol command [2-463](#)show idprom command [2-465](#)show interface rep command [2-477](#)show interfaces command [2-467](#)show interfaces counters command [2-475](#)show interfaces rep command [2-477](#)show interface transceivers command [2-479](#)show inventory command [2-482](#)show ip arp inspection command [2-483](#)show ipc command [2-512](#)show ip dhcp snooping binding command [2-488](#)

- show ip dhcp snooping command [2-487](#)
- show ip dhcp snooping database command [2-490, 2-492](#)
- show ip igmp profile command [2-497](#)
- show ip igmp snooping command [2-498](#)
- show ip igmp snooping command querier detail [2-503](#)
- show ip igmp snooping groups command [2-500](#)
- show ip igmp snooping mrouter command [2-502](#)
- show ip igmp snooping querier command [2-503](#)
- show ip igmp snooping querier detail command [2-503](#)
- show ip sla standards command [2-505](#)
- show ip sla twamp connection [2-435](#)
- show ip sla twamp connection command [2-506](#)
- show ip sla twamp session command [2-508](#)
- show ip source binding command [2-509](#)
- show ipv6 access-list command [2-516](#)
- show ipv6 dhcp conflict command [2-518](#)
- show ipv6 route updated command [2-519](#)
- show ip verify source command [2-510](#)
- show l2protocol-tunnel command [2-521](#)
- show lacp command [2-523](#)
- show link state group command [2-527](#)
- show location command [2-529](#)
- show logging onboard command [2-532](#)
- show mac access-group command [2-536](#)
- show mac address-table address command [2-539](#)
- show mac address-table aging time command [2-540](#)
- show mac address-table command [2-537](#)
- show mac address-table count command [2-542](#)
- show mac address-table dynamic command [2-544](#)
- show mac address-table interface command [2-546](#)
- show mac address-table learning command [2-548](#)
- show mac address-table move update command [2-549](#)
- show mac address-table notification command [2-50, 2-550, B-32](#)
- show mac address-table static command [2-552](#)
- show mac address-table vlan command [2-554](#)
- show monitor command [2-556](#)
- show mvr command [2-558](#)
- show mvr interface command [2-560](#)
- show mvr members command [2-562](#)
- show pagp command [2-564](#)
- show parser macro command [2-566](#)
- show platform acl command [C-2](#)
- show platform backup interface command [C-3](#)
- show platform cfm command [C-4](#)
- show platform configuration command [C-5](#)
- show platform dl command [C-6](#)
- show platform etherchannel command [C-7](#)
- show platform forward command [C-8](#)
- show platform frontend-controller command [C-10](#)
- show platform igmp snooping command [C-11](#)
- show platform ipc trace command [C-14](#)
- show platform ip multicast command [C-12](#)
- show platform ip unicast command [C-13](#)
- show platform ipv6 unicast command [C-15](#)
- show platform l2pt dm command [C-17](#)
- show platform layer4op command [C-18, C-40](#)
- show platform mac-address-table command [C-19](#)
- show platform messaging command [C-20](#)
- show platform monitor command [C-21](#)
- show platform mvr table command [C-22](#)
- show platform pm command [C-23](#)
- show platform policer cpu command [C-24](#)
- show platform port-asic command [C-28](#)
- show platform port-security command [C-32](#)
- show platform qos command [C-33](#)
- show platform resource-manager command [C-36](#)
- show platform snmp counters command [C-38](#)
- show platform spanning-tree synchronization command [C-39](#)
- show platform stp-instance command [C-41](#)
- show platform team command [C-42](#)
- show platform vlan command [C-44](#)
- show platform vlan mapping command [C-45](#)
- show policer aggregate command [2-568](#)
- show policer cpu uni-eni command [2-569](#)
- show policy-map command [2-572](#)
- show policy-map interface output fields [2-575](#)

- show port security command [2-577](#)
- show port-type command [2-580](#)
- show rep topology command [2-582](#)
- show sdm prefer command [2-585](#)
- show spanning-tree command [2-587](#)
- show storm-control command [2-593](#)
- show system mtu command [2-595](#)
- show udd command [2-597](#)
- show version command [2-600](#)
- show vlan access-map command [2-607](#)
- show vlan command [2-602](#)
- show vlan command, fields [2-604](#)
- show vlan filter command [2-608](#)
- show vlan mapping command [2-609](#)
- show vmpls command [2-611](#)
- shutdown command [2-613](#)
- shutdown threshold, Layer 2 protocol tunneling [2-245](#)
- shutdown vlan command [2-614](#)
- SNMP host, specifying [2-620](#)
- SNMP informs, enabling the sending of [2-616](#)
- snmp mib rep trap-rate command [2-615](#)
- snmp-server enable traps command [2-616](#)
- snmp-server host command [2-620](#)
- snmp trap mac-notification change command [2-624](#)
- SNMP traps
  - enabling MAC address notification trap [2-624](#)
  - enabling the MAC address notification feature [2-272](#)
  - enabling the sending of [2-616](#)
- software images
  - deleting [2-80](#)
  - downloading [2-9](#)
  - upgrading [2-9](#)
  - uploading [2-15](#)
- software version, displaying [2-600](#)
- source ports, MVR [2-312](#)
- SPAN
  - configuring [2-305](#)
  - debug messages, display [B-33](#)
  - displaying [2-556](#)
  - filter SPAN traffic [2-305](#)
  - sessions
    - add interfaces to [2-305](#)
    - displaying [2-556](#)
    - start new [2-305](#)
  - spanning-tree bpdudfilter command [2-626, 2-628](#)
  - spanning-tree bpduguard command [2-630](#)
  - spanning-tree cost command [2-632](#)
  - spanning-tree etherchannel command [2-634](#)
  - spanning-tree extend system-id command [2-636](#)
  - spanning-tree guard command [2-638](#)
  - spanning-tree link-type command [2-640](#)
  - spanning-tree loopguard default command [2-642](#)
  - spanning-tree mode command [2-644](#)
  - spanning-tree mst configuration command [2-646](#)
  - spanning-tree mst cost command [2-648](#)
  - spanning-tree mst forward-time command [2-650](#)
  - spanning-tree mst hello-time command [2-651](#)
  - spanning-tree mst max-age command [2-653](#)
  - spanning-tree mst max-hops command [2-655](#)
  - spanning-tree mst port-priority command [2-657](#)
  - spanning-tree mst pre-standard command [2-659](#)
  - spanning-tree mst priority command [2-660](#)
  - spanning-tree mst root command [2-662](#)
  - spanning-tree portfast (global configuration) command [2-666](#)
  - spanning-tree portfast (interface configuration) command [2-669](#)
  - spanning-tree port-priority command [2-664](#)
  - Spanning Tree Protocol
    - See STP
  - spanning-tree vlan command [2-671](#)
  - speed command [2-674](#)
  - SSH, configuring version [2-212](#)
  - static-access ports, configuring [2-681](#)
  - statistics, Ethernet group [2-385](#)

- sticky learning, enabling [2-696](#)
  - storm-control command [2-676](#)
  - STP
    - counters, clearing [2-56](#)
    - debug messages, display
      - MSTP [B-88](#)
      - optimized BPDUs handling [B-87](#)
      - spanning-tree activity [B-84](#)
      - switch shim [B-90](#)
      - transmitted and received BPDUs [B-86](#)
    - enabling on ENIs [2-626](#)
    - enabling protocol tunneling for [2-245](#)
    - EtherChannel misconfiguration [2-634](#)
    - extended system ID [2-636](#)
    - path cost [2-632](#)
    - protocol modes [2-644](#)
    - root port
      - loop guard [2-638](#)
      - preventing from becoming designated [2-638](#)
      - restricting which can be root [2-638](#)
      - root guard [2-638](#)
    - root switch
      - affects of extended system ID [2-636, 2-672](#)
      - hello-time [2-671](#)
      - interval between BDPUs messages [2-671](#)
      - interval between hello BDPUs messages [2-671](#)
      - max-age [2-671](#)
      - port priority for selection of [2-664](#)
      - primary or secondary [2-671](#)
      - switch priority [2-671](#)
    - state changes
      - blocking to forwarding state [2-669](#)
      - enabling BPDU filtering [2-628, 2-666](#)
      - enabling BPDU guard [2-630, 2-666](#)
      - enabling Port Fast [2-666, 2-669](#)
      - enabling timer to recover from error state [2-120](#)
      - forward-delay time [2-671](#)
      - length of listening and learning states [2-671](#)
      - shutting down Port Fast-enabled ports [2-666](#)
      - state information display [2-587](#)
      - VLAN options [2-660, 2-671](#)
    - SVIs, creating [2-149](#)
    - Switched Port Analyzer
      - See SPAN
    - switching characteristics
      - modifying [2-679](#)
      - returning to interfaces [2-679](#)
    - switchport access command [2-681](#)
    - switchport backup interface command [2-683](#)
    - switchport block command [2-687](#)
    - switchport command [2-679](#)
    - switchport host command [2-689](#)
    - switchport mode command [2-690](#)
    - switchport mode private-vlan command [2-693](#)
    - switchport port-security aging command [2-700](#)
    - switchport port-security command [2-696](#)
    - switchport private-vlan command [2-702](#)
    - switchport protected command [2-704](#)
    - switchports, displaying [2-467](#)
    - switchport trunk command [2-706](#)
    - switchport vlan mapping command [2-708](#)
    - system env temperature threshold yellow command [2-711](#)
    - system message logging, save message to flash [2-261](#)
    - system mtu command [2-712](#)
    - system resource templates [2-386](#)
- 
- ## T
- table-map command [2-715](#)
  - table-map configuration mode [2-715](#)
  - table maps
    - configuring [2-715](#)
    - displaying [2-596](#)
    - QoS [2-715](#)
  - tar files, creating, listing, and extracting [2-12](#)
  - TDR, running [2-717](#)
  - temperature information, displaying [2-445](#)
  - temperature status, displaying [2-445](#)

templates, system resources [2-386](#)  
 test cable-diagnostics tdr command [2-717](#)  
 traceroute mac command [2-719](#)  
 traceroute mac ip command [2-722](#)  
 traffic shaping, QoS [2-410](#)  
 trunking, VLAN mode [2-690](#)  
 trunk mode [2-690](#)  
 trunk ports [2-690](#)  
 tunnel ports, Layer 2 protocol, displaying [2-521](#)  
 type (boot loader) command [A-26](#)

## U

### UDLD

aggressive mode [2-724, 2-726](#)  
 debug messages, display [B-96](#)  
 enable globally [2-724](#)  
 enable per interface [2-726](#)  
 error recovery timer [2-120](#)  
 message timer [2-724](#)  
 normal mode [2-724, 2-726](#)  
 reset a shutdown interface [2-728](#)  
 status [2-597](#)

udld command [2-724](#)

udld port command [2-726](#)

udld reset command [2-728](#)

### UNI

bundling and multiplexing [2-136](#)  
 Ethernet [2-136](#)

unicast storm control [2-676](#)

uni count command [2-729](#)

### UniDirectional Link Detection

See UDLD

UNI ID, Ethernet [2-138](#)

uni-vlan command [2-731](#)

unknown multicast traffic, preventing [2-687](#)

unknown unicast traffic, preventing [2-687](#)

unset (boot loader) command [A-27](#)

### upgrading

software images [2-9](#)

monitoring status of [2-415](#)

user EXEC mode [1-2](#)

user network interface [2-352](#)

## V

version (boot loader) command [A-29](#)

violate-action command [2-733](#)

vlan access-map command [2-738](#)

VLAN access map configuration mode [2-738](#)

### VLAN access maps

actions [2-5](#)

displaying [2-607](#)

vlan command [2-735](#)

### VLAN configuration mode

commands [2-735](#)

description [1-4](#)

entering [2-735](#)

summary [1-2](#)

vlan dot1q tag native command [2-740](#)

vlan filter command [2-742](#)

VLAN filters, displaying [2-608](#)

VLAN ID range [2-735](#)

### VLAN ID translation

See VLAN mapping

### VLAN mapping

configuring [2-708](#)

described [2-709](#)

displaying [2-609](#)

### VLAN maps

applying [2-742](#)

creating [2-738](#)

defining [2-285](#)

displaying [2-607](#)

### VLAN Query Protocol

See VQP

## VLANs

- adding [2-735](#)
- configuring [2-735](#)
- debug messages, display
  - activation of [B-94](#)
  - VLAN IOS file system error tests [B-93](#)
  - VLAN manager activity [B-92](#)
- displaying configurations [2-602](#)
- extended-range [2-735](#)
- MAC addresses
  - displaying [2-554](#)
  - number of [2-542](#)
- normal-range [2-735](#)
- private [2-693](#)
  - configuring [2-359](#)
  - displaying [2-602](#)

See also private VLANs
- restarting [2-614](#)
- saving the configuration [2-735](#)
- shutting down [2-614](#)
- suspending [2-614](#)

## VMPS

- configuring servers [2-747](#)
- displaying [2-611](#)
- error recovery timer [2-121](#)
- reconfirming dynamic VLAN assignments [2-744](#)
- vmmps reconfirm (global configuration) command [2-745](#)
- vmmps reconfirm (privileged EXEC) command [2-744](#)
- vmmps retry command [2-746](#)
- vmmps server command [2-747](#)

## VQP

- and dynamic-access ports [2-682](#)
- clearing client statistics [2-59](#)
- displaying information [2-611](#)
- per-server retry count [2-746](#)
- reconfirmation interval [2-745](#)
- reconfirming dynamic VLAN assignments [2-744](#)

## VTP

- enabling
  - tunneling for [2-245](#)

---

**W**

## Weighted Tail Drop

See WTD

WTD, queue-limit command [2-364](#)