



Catalyst 3750 Metro Switch Command Reference

Cisco IOS Release 12.2(50)SE
March 2009

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-9645-07

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

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

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0812R)

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

Catalyst 3750 Metro Switch Command Reference
©2006-2009 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface **xix**

Audience **xix**

Purpose **xix**

Conventions **xix**

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 **1-3**

 config-vlan Mode **1-4**

 VLAN Configuration Mode **1-4**

 Line Configuration Mode **1-5**

Commands Changed in Cisco IOS 12.2(25)EY **1-5**

CHAPTER 2

Catalyst 3750 Metro Switch Cisco IOS Commands **2-1**

aaa accounting dot1x **2-1**

aaa authentication dot1x **2-3**

action **2-5**

archive download-sw **2-7**

archive tar **2-9**

archive upload-sw **2-12**

arp access-list **2-13**

auto qos voip **2-15**

bandwidth **2-20**

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	2-35
class-map	2-39
clear ip arp inspection log	2-41
clear ip arp inspection statistics	2-42
clear ip dhcp snooping	2-43
clear l2protocol-tunnel counters	2-45
clear lacp	2-46
clear mac address-table	2-47
clear mac address-table move update	2-48
clear pagp	2-49
clear rep counters	2-50
clear spanning-tree counters	2-51
clear spanning-tree detected-protocols	2-52
clear vmps statistics	2-53
clear vtp counters	2-54
cluster commander-address	2-55
cluster discovery hop-count	2-57
cluster enable	2-58
cluster holdtime	2-60
cluster member	2-61
cluster outside-interface	2-63
cluster run	2-64
cluster standby-group	2-65
cluster timer	2-67
cpu traffic qos	2-68
define interface-range	2-70
delete	2-72
deny	2-73
deny (ARP access-list configuration)	2-76
dot1x auth-fail max-attempts	2-78

dot1x auth-fail vlan	2-80
dot1x default	2-82
dot1x guest-vlan	2-83
dot1x host-mode	2-85
dot1x initialize	2-87
dot1x max-reauth-req	2-88
dot1x max-req	2-89
dot1x port-control	2-90
dot1x re-authenticate	2-92
dot1x reauthentication	2-93
dot1x system-auth-control	2-94
dot1x test eapol-capable	2-95
dot1x test timeout	2-96
dot1x timeout	2-97
dot1x violation-mode	2-99
duplex	2-101
errdisable detect cause	2-103
errdisable detect cause small-frame	2-105
errdisable recovery cause small-frame	2-107
errdisable recovery	2-108
ethernet evc	2-110
ethernet lmi	2-111
ethernet lmi ce-vlan map	2-113
ethernet oam remote-failure	2-115
ethernet uni	2-117
ethernet uni id	2-119
flowcontrol	2-120
interface port-channel	2-122
interface range	2-124
interface vlan	2-126
ip access-group	2-128
ip address	2-131
ip arp inspection filter vlan	2-133
ip arp inspection limit	2-135
ip arp inspection log-buffer	2-137

ip arp inspection trust	2-139
ip arp inspection validate	2-141
ip arp inspection vlan	2-143
ip arp inspection vlan logging	2-144
ip dhcp snooping	2-146
ip dhcp snooping binding	2-147
ip dhcp snooping database	2-149
ip dhcp snooping information option	2-151
ip dhcp snooping information option allowed-untrusted	2-153
ip dhcp snooping information option format remote-id	2-155
ip dhcp snooping limit rate	2-156
ip dhcp snooping trust	2-157
ip dhcp snooping verify	2-158
ip dhcp snooping vlan	2-159
ip dhcp snooping vlan information option format-type circuit-id string	2-160
ip igmp filter	2-162
ip igmp max-groups	2-164
ip igmp profile	2-166
ip igmp snooping	2-168
ip igmp snooping querier	2-170
ip igmp snooping report-suppression	2-172
ip igmp snooping vlan immediate-leave	2-174
ip igmp snooping vlan mrouter	2-175
ip igmp snooping vlan static	2-177
ip source binding	2-179
ip ssh	2-181
ip sticky-arp (global configuration)	2-183
ip sticky-arp (interface configuration)	2-185
ip verify source	2-187
ip vrf (global configuration)	2-188
ip vrf (interface configuration)	2-190
l2protocol-tunnel	2-192
l2protocol-tunnel cos	2-196
lACP port-priority	2-197
lACP system-priority	2-199

link state group	2-201
link state track	2-203
location (global configuration)	2-204
location (interface configuration)	2-206
logging event	2-208
logging file	2-209
mac access-group	2-211
mac access-list extended	2-213
mac address-table aging-time	2-215
mac address-table learning	2-216
mac address-table move update	2-218
mac address-table notification	2-220
mac address-table static	2-222
mac address-table static drop	2-223
macro apply	2-225
macro description	2-228
macro global	2-229
macro global description	2-232
macro name	2-233
match (access-map configuration)	2-235
match (class-map configuration)	2-237
mdix auto	2-240
mls qos	2-242
mls qos aggregate-policer	2-244
mls qos cos	2-246
mls qos dscp-mutation	2-248
mls qos enhanced	2-250
mls qos map	2-252
mls qos queue-set output buffers	2-255
mls qos queue-set output threshold	2-257
mls qos rewrite ip dscp	2-259
mls qos srr-queue input bandwidth	2-261
mls qos srr-queue input buffers	2-263
mls qos srr-queue input cos-map	2-265
mls qos srr-queue input dscp-map	2-267

mls qos srr-queue input priority-queue	2-269
mls qos srr-queue input threshold	2-271
mls qos srr-queue output cos-map	2-273
mls qos srr-queue output cpu-queue	2-275
mls qos srr-queue output dscp-map	2-277
mls qos trust	2-279
mls qos vlan-based	2-282
monitor session	2-283
mpls l2transport route	2-287
mpls ldp holdtime	2-289
mpls mtu	2-290
mvr (global configuration)	2-292
mvr (interface configuration)	2-295
oam protocol cfm svlan	2-299
pagp learn-method	2-300
pagp port-priority	2-302
permit	2-304
permit (ARP access-list configuration)	2-307
police	2-309
police aggregate	2-311
police cir	2-313
police cir percent	2-316
policy-map	2-320
port-channel load-balance	2-323
priority	2-325
priority-queue	2-327
private-vlan	2-329
private-vlan mapping	2-332
queue-limit	2-334
queue-set	2-336
random-detect	2-337
random-detect dscp	2-340
random-detect exponential-weighting-constant	2-344
random-detect precedence	2-347
rcommand	2-350

remote-span 2-352

renew ip dhcp snooping database 2-354

rep admin vlan 2-355

rep block port 2-356

rep lsl-age-timer 2-359

rep preempt delay 2-360

rep preempt segment 2-362

rep segment 2-363

rep stcn 2-366

reserved-only 2-368

rmon collection stats 2-369

sdm prefer 2-370

service instance 2-372

service password-recovery 2-373

service-policy (interface configuration) 2-375

service-policy (policy-map class) 2-378

set 2-380

setup 2-382

setup express 2-385

shape 2-387

show access-lists 2-389

show archive status 2-392

show arp access-list 2-393

show auto qos 2-394

show boot 2-398

show class-map 2-400

show cluster 2-401

show cluster candidates 2-403

show cluster members 2-405

show controllers cpu-interface 2-407

show controllers ethernet-controller 2-409

show controllers tcam 2-413

show cpu traffic qos 2-415

show dot1q-tunnel 2-416

show dot1x 2-417

[show dtp](#) 2-420

[show env](#) 2-422

[show errdisable detect](#) 2-423

[show errdisable flap-values](#) 2-425

[show errdisable recovery](#) 2-427

[show etherchannel](#) 2-429

[show ethernet service evc](#) 2-432

[show ethernet service instance](#) 2-433

[show ethernet service interface](#) 2-435

[show interfaces](#) 2-437

[show interfaces counters](#) 2-445

[show interfaces rep](#) 2-448

[show interfaces transceivers](#) 2-450

[show inventory](#) 2-453

[show ip arp inspection](#) 2-454

[show ip dhcp snooping](#) 2-458

[show ip dhcp snooping binding](#) 2-459

[show ip dhcp snooping database](#) 2-461

[show ip dhcp snooping statistics](#) 2-463

[show ip igmp profile](#) 2-466

[show ip igmp snooping](#) 2-467

[show ip igmp snooping groups](#) 2-469

[show ip igmp snooping mrouter](#) 2-471

[show ip igmp snooping querier](#) 2-473

[show ip source binding](#) 2-475

[show ip verify source](#) 2-476

[show l2protocol-tunnel](#) 2-478

[show lacp](#) 2-480

[show link state group](#) 2-484

[show location](#) 2-486

[show mac access-group](#) 2-488

[show mac address-table](#) 2-490

[show mac address-table address](#) 2-492

[show mac address-table aging-time](#) 2-494

[show mac address-table count](#) 2-496

show mac address-table dynamic	2-498
show mac address-table interface	2-500
show mac address-table learning	2-502
show mac address-table move update	2-503
show mac address-table multicast	2-505
show mac address-table notification	2-507
show mac address-table static	2-509
show mac address-table vlan	2-511
show mls qos	2-513
show mls qos aggregate-policer	2-514
show mls qos input-queue	2-515
show mls qos interface	2-517
show mls qos maps	2-520
show mls qos queue-set	2-523
show mls qos vlan	2-525
show monitor	2-526
show mpls l2transport vc	2-528
show mvr	2-532
show mvr interface	2-534
show mvr members	2-536
show pagp	2-538
show parser macro	2-540
show policy-map	2-543
show port-security	2-546
show rep topology	2-549
show sdm prefer	2-551
show setup express	2-553
show spanning-tree	2-554
show storm-control	2-560
show system mtu	2-562
show udd	2-563
show version	2-566
show vlan	2-568
show vlan access-map	2-573
show vlan filter	2-574

show vmps	2-575
show vtp	2-578
shutdown	2-583
shutdown vlan	2-584
small-frame violation rate	2-585
snmp mib rep trap-rate	2-587
snmp-server enable traps	2-588
snmp-server host	2-592
snmp trap mac-notification	2-597
spanning-tree backbonefast	2-598
spanning-tree bpdupfilter	2-599
spanning-tree bpduguard	2-601
spanning-tree cost	2-603
spanning-tree etherchannel guard misconfig	2-605
spanning-tree extend system-id	2-607
spanning-tree guard	2-608
spanning-tree link-type	2-610
spanning-tree loopguard default	2-612
spanning-tree mode	2-614
spanning-tree mst configuration	2-616
spanning-tree mst cost	2-618
spanning-tree mst forward-time	2-620
spanning-tree mst hello-time	2-621
spanning-tree mst max-age	2-622
spanning-tree mst max-hops	2-623
spanning-tree mst pre-standard	2-625
spanning-tree mst port-priority	2-626
spanning-tree mst priority	2-628
spanning-tree mst root	2-629
spanning-tree port-priority	2-631
spanning-tree portfast (global configuration)	2-633
spanning-tree portfast (interface configuration)	2-635
spanning-tree uplinkfast	2-637
spanning-tree vlan	2-639
speed	2-642

srr-queue bandwidth limit	2-644
srr-queue bandwidth shape	2-646
srr-queue bandwidth share	2-648
storm-control	2-650
switchport	2-653
switchport access	2-655
switchport backup interface	2-657
switchport block	2-664
switchport host	2-665
switchport mode	2-666
switchport mode private-vlan	2-669
switchport nonegotiate	2-671
switchport port-security	2-673
switchport port-security aging	2-677
switchport priority extend	2-679
switchport private-vlan	2-681
switchport protected	2-683
switchport trunk	2-684
switchport vlan mapping	2-688
switchport voice vlan	2-691
system mtu	2-693
traceroute mac	2-695
traceroute mac ip	2-698
trust	2-700
udld (global configuration)	2-702
udld (interface configuration)	2-704
udld reset	2-706
uni count	2-707
vlan (global configuration)	2-709
vlan (VLAN configuration)	2-715
vlan access-map	2-721
vlan database	2-723
vlan filter	2-726
vmps reconfirm (privileged EXEC)	2-728
vmps reconfirm (global configuration)	2-729

[vmps retry](#) **2-730**
[vmps server](#) **2-731**
[vtp \(global configuration\)](#) **2-733**
[vtp \(VLAN configuration\)](#) **2-737**
[xconnect](#) **2-741**

APPENDIX A

Catalyst 3750 Metro Switch Boot Loader Commands **A-1**

[boot](#) **A-2**
[cat](#) **A-4**
[copy](#) **A-5**
[delete](#) **A-6**
[dir](#) **A-7**
[flash_init](#) **A-9**
[format](#) **A-10**
[fsck](#) **A-11**
[help](#) **A-12**
[memory](#) **A-13**
[mkdir](#) **A-15**
[more](#) **A-16**
[rename](#) **A-17**
[reset](#) **A-18**
[rmdir](#) **A-19**
[set](#) **A-20**
[type](#) **A-23**
[unset](#) **A-24**
[version](#) **A-26**

APPENDIX B

Catalyst 3750 Metro Switch Debug Commands **B-1**

[debug auto qos](#) **B-2**
[debug backup](#) **B-4**
[debug cluster](#) **B-5**
[debug dot1x](#) **B-7**
[debug dtp](#) **B-8**
[debug etherchannel](#) **B-9**
[debug ethernet service](#) **B-10**

debug interface	B-12
debug ip dhcp snooping	B-13
debug ip igmp filter	B-14
debug ip igmp max-groups	B-15
debug ip igmp snooping	B-16
debug ip verify source packet	B-17
debug lacp	B-18
debug mac-notification	B-19
debug matm	B-20
debug matm move update	B-21
debug monitor	B-22
debug mpls atom	B-23
debug mpls l2transport vlan	B-24
debug mvrdbg	B-25
debug nvram	B-26
debug pagp	B-27
debug platform acl	B-28
debug platform cfm	B-29
debug platform backup interface	B-30
debug platform cpu-queues	B-31
debug platform dot1x	B-33
debug platform etherchannel	B-34
debug platform fallback-bridging	B-35
debug platform forw-tcam	B-36
debug platform ip arp inspection	B-37
debug platform ip igmp snooping	B-38
debug platform ip multicast	B-40
debug platform ip unicast	B-42
debug platform led	B-44
debug platform matm	B-45
debug platform messaging application	B-46
debug platform mpls	B-47
debug platform phy	B-48
debug platform pm	B-49
debug platform port-asic	B-51

debug platform port-security	B-52
debug platform qos-acl-tcam	B-53
debug platform remote-commands	B-54
debug platform rep	B-55
debug platform resource-manager	B-56
debug platform snmp	B-57
debug platform span	B-58
debug platform supervisor-asic	B-59
debug platform sw-bridge	B-60
debug platform tcam	B-61
debug platform udd	B-63
debug platform vlan	B-64
debug pm	B-65
debug port-security	B-67
debug rep	B-68
debug qos-manager	B-69
debug spanning-tree	B-70
debug spanning-tree backbonefast	B-72
debug spanning-tree bpd	B-73
debug spanning-tree bpd-opt	B-74
debug spanning-tree mstp	B-75
debug spanning-tree switch	B-77
debug spanning-tree uplinkfast	B-79
debug sw-vlan	B-80
debug sw-vlan ifs	B-82
debug sw-vlan notification	B-83
debug sw-vlan vtp	B-84
debug udd	B-86
debug vqpc	B-88
debug xconnect	B-89

APPENDIX C

Catalyst 3750 Metro Switch Show Platform Commands C-1

show platform acl	C-2
show platform cfm	C-3
show platform configuration	C-4

show platform etherchannel	C-5
show platform forward	C-6
show platform ip igmp snooping	C-8
show platform ip multicast	C-10
show platform ip policy	C-11
show platform ip unicast	C-12
show platform ipc trace	C-14
show platform layer4op	C-15
show platform mac-address-table	C-16
show platform messaging	C-17
show platform monitor	C-18
show platform mvr table	C-19
show platform pm	C-20
show platform port-asic	C-22
show platform port-security	C-26
show platform qos	C-27
show platform resource-manager	C-28
show platform snmp counters	C-30
show platform spanning-tree	C-31
show platform stp-instance	C-32
show platform tb	C-33
show platform tcam	C-34
show platform vlan	C-37

APPENDIX D
Acknowledgments for Open-Source Software D-1

INDEX



Preface

Audience

This guide is for the networking professional using the Cisco IOS command-line interface (CLI) to manage the Catalyst 3750 Metro 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. Before using this guide, you should have experience working with the concepts and terminology of Ethernet and local area networking.

Purpose

The Catalyst 3750 Metro switch is supported by a set of enterprise-class features, including Layer 2+ features such as access control lists (ACLs) and quality of service (QoS) and Layer 3 features such as IP unicast routing, IP multicast routing, and fallback bridging. It also includes features for the service provider, including multiprotocol label switching (MPLS), Ethernet over MPLS (EoMPLS), hierarchical QoS, and 802.1Q tunneling.

This guide provides the information you need about the commands that have been created or changed for use with the Catalyst 3750 Metro switches. 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 that you might encounter. For more information, see the system message guide for this release.

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

Conventions

This publication uses these conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in **boldface** text.
- Arguments for which you supply values are in *italic*.

- Square brackets ([]) means optional elements.
- Braces ({ }) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

Interactive examples use these conventions:

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

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



Note

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



Caution

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

Related Publications

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

http://www.cisco.com/en/US/products/hw/switches/ps5532/tsd_products_support_series_home.html



Note

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

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

- *Release Notes for the Catalyst 3750 Metro Switch*
- *Catalyst 3750 Metro Switch Software Configuration Guide*
- *Catalyst 3750 Metro Switch Command Reference*
- *Catalyst 3750 Metro Switch System Message Guide*
- *Catalyst 3750 Metro Switch Hardware Installation Guide*
- *Cisco Small Form-Factor Pluggable Modules Installation Notes*

- 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

- *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 Catalyst 3750 Metro 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 of the commands that support these features, see [Chapter 2, “Catalyst 3750 Metro Switch Cisco IOS Commands.”](#) For information on the boot loader commands, see [Appendix A, “Catalyst 3750 Metro Switch Boot Loader Commands.”](#) For information on the **debug** commands, see [Appendix B, “Catalyst 3750 Metro Switch Debug Commands.”](#) For information on the **show platform** commands, see [Appendix C, “Catalyst 3750 Metro 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.

CLI Command Modes

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

These are the main command modes for the switch:

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

[Table 1-1](#) 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 logout command. To enter privileged EXEC mode, enter the enable command.
Privileged EXEC	From user EXEC mode, enter the enable command.	Switch#	To exit to user EXEC mode, enter the disable command. To enter global configuration mode, enter the configure command.
Global configuration	From privileged EXEC mode, enter the configure command.	Switch(config)#	To exit to privileged EXEC mode, enter the exit or end command, or press Ctrl-Z . To enter interface configuration mode, enter the interface configuration command.
Interface configuration	From global configuration mode, specify an interface by entering the interface command followed by an interface identification.	Switch(config-if)#	To exit to privileged EXEC mode, enter the end command, or press Ctrl-Z . To exit to global configuration mode, enter the exit command.
Config-vlan	In global configuration mode, enter the vlan <i>vlan-id</i> command.	Switch(config-vlan)#	To exit to global configuration mode, enter the exit command. To return to privileged EXEC mode, enter the end command, or press Ctrl-Z .
VLAN configuration	From privileged EXEC mode, enter the vlan database command.	Switch(vlan)#	To exit to privileged EXEC mode, enter the exit command.
Line configuration	From global configuration mode, specify a line by entering the line command.	Switch(config-line)#	To exit to global configuration mode, enter the exit command. To return to privileged EXEC mode, enter the end command, or press Ctrl-Z .

User EXEC Mode

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

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

```
Switch# ?
```

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

Global Configuration Mode

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

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

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

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

This example shows you how to access global configuration mode:

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

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

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

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

config-vlan Mode

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

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

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

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

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

For extended-range VLANs, all characteristics except the maximum transmission unit (MTU) size must remain at the default setting.

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

VLAN Configuration Mode

You can use the VLAN configuration commands to create or modify VLAN parameters for VLAN IDs 1 to 1005.

Enter the **vlan database** privileged EXEC command to access VLAN configuration mode:

```
Switch# vlan database  
Switch(vlan)#
```

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

```
Switch(vlan)# ?
```

To return to privileged EXEC mode, enter the **abort** VLAN configuration command to abandon the proposed database. Otherwise, enter **exit** to implement the proposed new VLAN database and to return to privileged EXEC mode. When you enter **exit** or **apply**, the configuration is saved in the VLAN database; configuration from VLAN configuration mode cannot be saved in the switch configuration file.

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 view 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**.

Commands Changed in Cisco IOS 12.2(25)EY

Table 1-2 lists describes the commands that have the same function but different syntax than they did in software releases before Cisco IOS Release 12.2(25)EY.

Table 1-2 *Commands Changed*

Releases earlier than Cisco IOS Release 12.2(25)EY	Cisco IOS Release 12.2(25)EY or later	Description
debug autoqos	debug auto qos	Enables debugging of the auto-QoS ¹ feature.
xconnect {destination vc-id}	xconnect {destination vc-id encapsulation mpls}	Routes a Layer 2 packets over a specified point-to-point virtual connection.

1. auto-QoS = automatic quality of service



CHAPTER 2

Catalyst 3750 Metro 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 802.1x sessions. Use the **no** form of this command to disable 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

name	Name of a server group. This is optional when you enter it after the broadcast group and group keywords.
default	Use the accounting methods that follow as the default list for accounting services.
start-stop	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.
broadcast	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.
group	Specify the server group to be used for accounting services. These are valid server group names: • name—Name of a server group. • radius—List of all RADIUS hosts. • tacacs+—List of all TACACS+ hosts. The group keyword is optional when you enter it after the broadcast group and group keywords. You can enter more than optional group keyword.
radius	(Optional) Enable RADIUS authorization.
tacacs+	(Optional) Enable TACACS+ accounting.

■ **aaa accounting dot1x****Defaults**

AAA accounting is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)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 802.1x RADIUS accounting on an interface.

Examples

This example shows how to configure 802.1x accounting:

```
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
aaa accounting dot1x	Specifies one or more AAA methods for use on interfaces running 802.1x.
dot1x reauthentication	Enables or disables periodic reauthentication.
dot1x test	Sets the number of seconds between re-authentication attempts.
capo1-capable	
reauth-period	

aaa authentication dot1x

Use the **aaa authentication dot1x** global configuration command to specify one or more authentication, authorization, and accounting (AAA) methods for use on ports running IEEE 802.1x. Use the **no** form of this command to disable authentication.

aaa authentication dot1x {default} method1 [method2...]

no aaa authentication dot1x {default}

Syntax Description

default	Use the listed authentication methods that follow this argument as the default list of methods when a user logs in.
<i>method1</i> [<i>method2...</i>]	At least one of the these keywords: enable—Use the enable password for authentication. group radius—Use the list of all RADIUS servers for authentication. line—Use the line password for authentication. local—Use the local username database for authentication. local-case—Use the case-sensitive local username database for authentication. none—Use no authentication. The client is automatically authenticated by the switch without using the information supplied by the client.



Note

Though visible in the command-line help strings, the **group tacacs+** keyword is not supported.

Defaults

No authentication is performed.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The *method* argument identifies the list of methods that the authentication algorithm tries in the given sequence to validate the password provided by the client. The only method that is truly 802.1x-compliant is the **group radius** method, in which the client data is validated against a RADIUS authentication server. The remaining methods enable AAA to authenticate the client by using locally configured data. For example, the **local** and **local-case** methods use the username and password that are saved in the configuration file. The **enable** and **line** methods use the **enable** and **line** passwords for authentication.

If you specify **group radius**, you must configure the RADIUS server by entering the **radius-server host** global configuration command.

If you are not using a RADIUS server, you can use the **local** or **local-case** methods, which access the local username database to perform authentication. By specifying the **enable** or **line** methods, you can supply the clients with a password to provide access to the switch.

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 authentication list for 802.1x. This authentication first tries to contact a RADIUS server. If this action returns an error, the user is allowed access with no authentication.

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius none
```

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

Related Commands

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

drop	Drop the packet when the specified conditions are matched.
forward	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
12.1(14)AX	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
	access-list {deny permit}	Configures a standard numbered ACL. For syntax information, select Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands .
	ip access-list	Creates a named access list. For syntax information, select Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands .
	mac access-list extended	Creates a named MAC address access list.
	match (access-map configuration)	Defines the match conditions for a VLAN map.
	show vlan access-map	Displays the VLAN access maps created on the switch.
	vlan access-map	Creates a VLAN access map.

archive download-sw

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

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

Syntax Description	
/force-reload	Unconditionally force a system reload after successfully downloading the software image.
/imageonly	Download only the Cisco IOS software image.
/leave-old-sw	Keep the old software version after a successful download.
/no-set-boot	Do not alter the setting of the BOOT environment variable to point to the new software image after it is successfully downloaded.
/overwrite	Overwrite the software image in flash memory with the downloaded one.
/reload	Reload the system after successfully downloading the image unless the configuration has been changed and not been saved.
/safe	Keep the current software image; do not delete it to make room for the new software image before the new image is downloaded. The current image is deleted after the download.
<i>source-url</i>	The source URL alias for a 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]/image-name.tar - The syntax for the Remote Copy Protocol (RCP): rcp:[[/username@location]/directory]/image-name.tar - The syntax for the TFTP: tftp:[[/location]/directory]/image-name.tar The <i>image-name.tar</i> is the software image to download and install on the switch.



Note

Though visible in the command-line help strings, the **no-version-check** keyword is not supported.

Defaults

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

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

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

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

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines 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 2-72](#).

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

archive tar

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

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

Syntax Description

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

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

For *destination-url*, specify 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 <i>source-url</i>	Display the contents of an existing tar file to the screen. For <i>source-url</i>, 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 <i>tar-filename.tar</i> is the tar file to display.
/xtract <i>source-url</i> flash: <i>/file-url [dir/file...]</i>	Extract files from a tar file to the local file system. For <i>source-url</i>, specify the source URL alias for the local file system. These options are supported: - The syntax for the local flash file system: flash: - The syntax for the FTP: ftp:[[//username[:password]@location]/directory]/tar-filename.tar - The syntax for the RCP: rcp:[[//username@location]/directory]/tar-filename.tar - The syntax for the TFTP: tftp:[[//location]/directory]/tar-filename.tar The <i>tar-filename.tar</i> is the tar file from which to extract. For flash:<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.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	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 *image-tv0-m.tar* file that is in flash memory. The contents of the tar file are displayed on the screen.

```
Switch# archive tar /table flash:image-tv0-m.tar
info (219 bytes)
image-tv0-mz-121/ (directory)
image-tv0-mz-121/html/ (directory)
image-tv0-mz-121/html/foo.html (0 bytes)
image-tv0-mz-121/image-tv0-mz-121.bin (610856 bytes)
image-tv0-mz-121/info (219 bytes)
info.ver (219 bytes)
```

This example shows how to display only the *image-tv0-mz-121/html* directory and its contents:

```
Switch# archive tar /table flash:image-tv0-m.tar image-tv0-mz-121/html
image-tv0-mz-121/html/ (directory)
image-tv0-mz-121/html/foo.html (0 bytes)
```

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

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

Related Commands

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

archive upload-sw

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

archive upload-sw *destination-url*

Syntax Description	<i>destination-url</i>	The destination URL alias for a 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]/image-name.tar - The syntax for the Remote Copy Protocol (RCP): rcp:[[/username@location]/directory]/image-name.tar - The syntax for the TFTP: tftp:[[/location]/directory]/image-name.tar The <i>image-name.tar</i> is the name of software image to be stored on the server.

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

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	The files are uploaded in this sequence: the Cisco IOS image and the info file. 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: <pre>Switch# archive upload-sw tftp://172.20.140.2/test-image.tar</pre>

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

arp access-list

Use the **arp access-list** global configuration command on the switch stack or on a standalone switch 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*

This command is available only if your switch is running the enhanced multilayer image (EMI).

Syntax Description	<i>acl-name</i>	Name of the ACL.

Defaults	No ARP access lists are defined.

Command Modes	Global configuration

Command History	Release	Modification
	12.2(25)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 2-76](#).
- **exit:** exits ARP access-list configuration mode.
- **no:** negates a command or returns to default settings.
- **permit:** specifies packets to forward. For more information, see the [“permit \(ARP access-list configuration\)” section on page 2-307](#).

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 00001.0000.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
deny (ARP access-list configuration)	Denies an ARP packet based on matches compared against the DHCP bindings.
ip arp inspection filter vlan	Permits ARP requests and responses from a host configured with a static IP address.
permit	Permits an ARP packet based on matches compared against the DHCP bindings.
show arp access-list	Displays detailed information about ARP access lists.

auto qos voip

Use the **auto qos voip** interface configuration command to automatically configure quality of service (QoS) for voice over IP (VoIP) within a QoS domain. Use the **no** form of this command to return to the default setting.

auto qos voip { **cisco-phone** | **cisco-softphone** | **trust** }

no auto qos voip [**cisco-phone** | **cisco-softphone** | **trust**]

Syntax Description

cisco-phone	Identify this port as connected to a Cisco IP phone, and automatically configure QoS for VoIP. The QoS labels of inbound packets are trusted only when the phone is detected.
cisco-softphone	Identify this port as connected to a device running the Cisco SoftPhone, and automatically configure QoS for VoIP.
trust	Identify this port as connected to a trusted switch or router, and automatically configure QoS for VoIP. The QoS labels of inbound packets are trusted. For nonrouted ports, the class of service (CoS) value of the inbound packet is trusted. For routed ports, the Differentiated Services Code Point (DSCP) value is trusted.

Defaults

Auto-QoS is disabled on the port.

When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, to assign packet labels, and to configure the ingress queues and egress queue-sets. [Table 2-1](#) shows the default settings.

Table 2-1 Traffic Types, Packet Labels, and Queues

	VoIP Data Traffic	VoIP Control Traffic	Routing Protocol Traffic	STP ¹ BPDU ² Traffic	Real-Time Video Traffic	All Other Traffic	
DSCP ³	46	24, 26	48	56	34	–	
CoS ⁴	5	3	6	7	3	–	
CoS-to-Ingress Queue Map	2, 3, 4, 5, 6, 7 (queue 2)					0, 1 (queue 1)	
CoS-to-Egress Queue Map	5 (queue 1)	3, 6, 7 (queue 2)			4 (queue 3)	2 (queue 3)	0, 1 (queue 4)

1. STP = Spanning Tree Protocol

2. BPDU = bridge protocol data unit

3. DSCP = Differentiated Services Code Point

4. CoS = class of service

[Table 2-2](#) shows the generated auto-QoS configuration for the ingress queues.

Table 2-2 Auto-QoS Configuration for the Ingress Queues

Ingress Queue	Queue Number	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size
SRR ¹ shared	1	0, 1	81 percent	67 percent
Priority	2	2, 3, 4, 5, 6, 7	19 percent	33 percent

1. SRR = shaped round robin. Ingress queues support shared mode only.

Table 2-3 shows the generated auto-QoS configuration for the egress queue-set.

Table 2-3 Auto-QoS Configuration for the Egress Queue-Set

Egress Queue ¹	Queue Number in the Queue-Set	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size
Priority (shaped)	1	5	10 percent	10 percent
SRR shared	2	3, 6, 7	10 percent	10 percent
SRR shared	3	2, 4	60 percent	26 percent
SRR shared	4	0, 1	20 percent	54 percent

1. On an enhanced-services (ES) port, the **srr-queue bandwidth shape** interface configuration command is not part of the generated **auto qos voip** command list.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.
12.2(25)EY	The cisco-softphone keyword was added, and the generated auto-QoS configuration changed.

Usage Guidelines

Use this command to configure the QoS appropriate for VoIP traffic within the QoS domain. The QoS domain includes the switch, the interior of the network, and edge devices that can classify inbound traffic for QoS.

In releases earlier than Cisco IOS Release 12.2(25)EY, auto-QoS configures the switch only for VoIP with Cisco IP Phones on switch ports.

In Cisco IOS Release 12.2(25)EY or later, auto-QoS configures the switch for VoIP with Cisco IP Phones on switch and routed ports and for VoIP with devices running the Cisco SoftPhone application. These releases support only Cisco IP SoftPhone Version 1.3(3) or later. Connected devices must use Cisco Call Manager Version 4 or later.

To take advantage of the auto-QoS defaults, you should enable auto-QoS before you configure other QoS commands. You can fine-tune the auto-QoS configuration *after* you enable auto-QoS.

**Note**

The switch applies the auto-QoS-generated commands as if the commands were entered from the command-line interface (CLI). An existing user configuration can cause the application of the generated commands to fail, or the user configuration might be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the switch without saving the current configuration to memory. If the generated commands are not applied, the previous running configuration is restored.

If this is the first port on which you have enabled auto-QoS, the auto-QoS-generated global configuration commands are executed, followed by the interface configuration commands. If you enable auto-QoS on another port, only the auto-QoS-generated interface configuration commands for that port are executed.

When you enable the auto-QoS feature on the first port, these automatic actions occur:

- QoS is globally enabled (**mls qos** global configuration command), and other global configuration commands are added.
- When you enter the **auto qos voip cisco-phone** interface configuration command on a port at the edge of the network that is connected to a Cisco IP phone, the switch enables the trusted boundary feature. The switch uses the Cisco Discovery Protocol (CDP) to detect the presence or absence of a Cisco IP phone. When a Cisco IP phone is detected, the ingress classification on the port is set to trust the QoS label received in the packet. When a Cisco IP phone is absent, the ingress classification is set to not trust the QoS label in the packet. The switch configures ingress queues and the egress queue-set on the port according to the settings in [Table 2-2](#) and [Table 2-3](#).
- When you enter the **auto qos voip cisco-softphone** interface configuration command on a port at the edge of the network that is connected to a device running the Cisco SoftPhone, the switch uses policing to decide whether a packet is in or out of profile and to specify the action on the packet. If the packet does not have a DSCP value of 24, 26, or 46 or is out of profile, the switch changes the DSCP value to 0. The switch configures ingress and egress queues on the port according to the settings in [Table 2-2](#) and [Table 2-3](#).
- When you enter the **auto qos voip trust** interface configuration command on a port connected to the interior of the network, the switch trusts the CoS value for nonrouted ports or the DSCP value for routed ports in ingress packets (the assumption is that traffic has already been classified by other edge devices). The switch configures the ingress queues and the egress queue-set on the port according to the settings in [Table 2-2](#) and [Table 2-3](#).

You can enable auto-QoS on static, dynamic-access, voice VLAN access, and trunk ports. When enabling auto-QoS with a Cisco IP Phone on a routed port, you must assign a static IP address to the IP phone.

To display the QoS commands that are automatically generated when auto-QoS is enabled or disabled, enable debugging before you enable auto-QoS. Use the **debug auto qos** privileged EXEC command to enable auto-QoS debugging. For more information, see the [debug auto qos](#) command.

**Note**

When a device running Cisco SoftPhone is connected to a switch or routed port, the switch supports only one Cisco SoftPhone application per port.

After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes *AutoQoS* in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy map or policer. To use the new policy map instead of the generated one, remove the generated policy map from the interface, and apply the new policy map.

To disable auto-QoS on a port, use the **no auto qos voip** interface configuration command. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled and you enter the **no auto qos voip** command, auto-QoS is considered disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration). You can use the **no mls qos** global configuration command to disable the auto-QoS-generated global configuration commands. With QoS disabled, there is no concept of trusted or untrusted ports because the packets are not modified (the CoS, DSCP, and IP precedence values in the packet are not changed). Traffic is switched in pass-through mode (packets are switched without any rewrites and classified as best effort without any policing).

Examples

This example shows how to enable auto-QoS on a port and to trust the QoS labels received in inbound packets when the switch or router connected to a port is a trusted device:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# auto qos voip trust
```

You can verify your settings by entering the **show auto qos interface interface-id** privileged EXEC command.

Related Commands

Command	Description
debug auto qos	Enables debugging of the auto-QoS feature.
mls qos cos	Defines the default CoS value of a port or assigns the default CoS to all inbound packets on the port.
mls qos map {cos-dscp dscp1 ... dscp8 dscp-cos dscp-list to cos}	Defines the CoS-to-DSCP map or the DSCP-to-CoS map.
mls qos queue-set output buffers	Allocates buffers to a queue-set.
mls qos srr-queue input bandwidth	Assigns SRR weights to an ingress queue.
mls qos srr-queue input buffers	Allocates the buffers between the ingress queues.
mls qos srr-queue input cos-map	Maps CoS values to an ingress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue input dscp-map	Maps DSCP values to an ingress queue or maps DSCP values to a queue and to a threshold ID.
mls qos srr-queue input priority-queue	Configures the ingress priority queue and guarantees bandwidth.
mls qos srr-queue output cos-map	Maps CoS values to an egress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue output dscp-map	Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID.
mls qos trust	Configures the port trust state.
queue-set	Maps a port to a queue-set.
show auto qos	Displays the initial configuration that is generated by the auto-QoS feature.
show mls qos interface	Displays QoS information at the port level.

Command	Description
srr-queue bandwidth shape	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a standard port.
srr-queue bandwidth share	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

bandwidth

Use the **bandwidth** policy-map class configuration command to specify or modify the minimum bandwidth provided to a class belonging to a hierarchical policy map attached to an enhanced-services (ES) port. Use the **no** form of this command to return to the default setting.

bandwidth { *bandwidth-kbps* | **percent** *percent* }

no bandwidth

Syntax Description	<i>bandwidth-kbps</i>	Amount of bandwidth in kbps assigned to the class. The range is 200 to 2000000. Allocate the bandwidth in 100-kbps increments; otherwise, the software rounds down the bandwidth to the nearest 100-kbps increment.
	percent <i>percent</i>	Percentage of available bandwidth assigned to the parent class. The range is 1 to 100.

Defaults No bandwidth is specified.

Command Modes Policy-map class configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.
	12.2(25)EY	Hierarchical service policies can be applied to inbound traffic received on an ES port.

Usage Guidelines Use the **bandwidth** command only in a hierarchical policy map attached to an ES port. This command is not valid for the class-default class in a physical-level policy map.

Use the **bandwidth** command when you configure a policy map for a class defined by the **class-map** global configuration command. The **bandwidth** command specifies the minimum bandwidth for traffic in that class when there is traffic congestion in the switch. If the switch is not congested, the class receives more bandwidth than you specify with this command. Class-based weighted fair queueing (CBWFQ) derives the weight for packets belonging to the class from the bandwidth allocated to the class. CBWFQ then uses the weight to ensure that the queue for the class is serviced fairly.



Note

It is important to remember that hard bandwidth guarantees might not be provided and that only relative bandwidths are assured. That is, class bandwidths are always proportional to the specified percentages of the port bandwidth. When the link bandwidth is fixed, class bandwidth guarantees are in proportion to the configured percentages.

These restrictions apply to the **bandwidth** command:

- If the **percent** keyword is used, the sum of the class bandwidth percentages within a single policy map cannot exceed 99 percent. Percentage calculations are based on the bandwidth available at the parent class (or the port if it is the parent).
- The amount of bandwidth available to a class is dependent on the amount of bandwidth reserved by the parent class.
- The amount of bandwidth configured should be large enough to accommodate Layer 2 overhead.
- A policy map can have all the class bandwidths specified in either kbps or in percentages, but not a mix of both. You cannot specify bandwidth in kbps in a child policy (configured through the **service-policy** policy-map class configuration command) and then specify bandwidth as a percentage in the parent policy.
- You cannot use the **bandwidth** command for the class-default class map in a physical-level policy map.
- Though visible in the command-line interface, the **max-reserved-bandwidth** interface configuration command and the **bandwidth** interface configuration command are not supported on the ES ports.

When you configure the **bandwidth** command in a class policy, you must also configure the **bandwidth** or **shape** policy-map class configuration command in the parent VLAN-level policy.

You must configure the **bandwidth** or the **shape** policy-map class configuration command before you configure either the **queue-limit** or the **random-detect** policy-map class configuration command in a class policy.

You cannot use the **bandwidth**, **queue-limit**, **random-detect**, and the **shape** policy-map class configuration commands with the **priority** policy-map class configuration command in the same class within the same policy map. However, you can use these commands in the same policy map.

When you use the **service-policy** interface configuration command to attach the policy map containing class configurations to an ES port, the switch determines the available bandwidth.

Examples

This example shows how to set the minimum bandwidth to 2000 kbps for a class called *silver-class*. The class already exists in the switch configuration.

```
Switch(config)# policy-map polmap6
Switch(config-pmap)# class silver-class
Switch(config-pmap-c)# bandwidth 2000
```

This example shows how to guarantee 30 percent of the bandwidth for *class1* and 25 percent of the bandwidth for *class2* when CBWFQ is configured. A policy map with two classes is created and is then attached to an ES port.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# bandwidth percent 25
Switch(config-pmap-c)# exit
Switch(config-pmap)# end
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# service-policy input policy1
```

This example shows how bandwidth is guaranteed if low-latency queueing (LLQ) and CBWFQ are configured. In this example, LLQ is enabled in a class called *voice1*.

```
Switch(config)# policy-map policy1
```

```

Switch(config-pmap) # class class1
Switch(config-pmap-c) # bandwidth percent 50
Switch(config-pmap-c) # exit
Switch(config-pmap) # class class2
Switch(config-pmap-c) # bandwidth percent 25
Switch(config-pmap-c) # exit
Switch(config-pmap) # class voice1
Switch(config-pmap-c) # priority
Switch(config-pmap-c) # exit
Switch(config-pmap) # end
Switch(config) # interface gigabitethernet1/1/1
Switch(config-if) # service-policy output policy1

```

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

Related Commands

Command	Description
class	Specifies the name of the class whose traffic policy you want to create or change.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
priority	Enables the strict-priority queue and gives priority to a class of traffic belonging to a policy map attached to an ES port.
queue-limit	Configures the maximum threshold for tail drop in a policy map attached to an ES port.
random-detect	Configures Weighted Random Early Detection (WRED) in a policy map attached to an ES port.
service-policy (policy-map class)	Creates a service policy as a quality of service (QoS) policy within a policy map.
shape	Enables traffic shaping in a policy map attached to an ES port.
show policy-map	Displays QoS policy maps.

boot config-file

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

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

no boot config-file

Syntax Description

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

Defaults

The default configuration file is flash:config.text.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

This command changes the setting of the CONFIG_FILE environment variable. For more information, see [Appendix A, “Catalyst 3750 Metro Switch Boot Loader Commands.”](#)

Related Commands

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

boot enable-break

Use the **boot enable-break** global configuration command 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
12.1(14)AX	This command was introduced.

Usage Guidelines

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



Note

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

This command changes the setting of the ENABLE_BREAK environment variable. For more information, see [Appendix A, “Catalyst 3750 Metro Switch Boot Loader Commands.”](#)

Related Commands

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

boot helper

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

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

no boot helper

Syntax Description	<i>filesystem:</i>	Alias for a flash file system. Use flash: 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
	12.1(14)AX	This command was introduced.

Usage Guidelines	This variable is used only for internal development and testing.
	Filenames and directory names are case sensitive.
	This command changes the setting of the HELPER environment variable. For more information, see Appendix A, “Catalyst 3750 Metro Switch Boot Loader Commands.”

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

boot helper-config-file

Use the **boot helper-config-file** global configuration command to specify the name of the configuration file to be used by the helper image. If this is not set, the file specified by the CONFIG_FILE environment variable is used by all versions of software 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 flash: 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
	12.1(14)AX	This command was introduced.

Usage Guidelines	This variable is used only for internal development and testing.
	Filenames and directory names are case sensitive.
	This command changes the setting of the HELPER_CONFIG_FILE environment variable. For more information, see Appendix A, “Catalyst 3750 Metro Switch Boot Loader Commands.”

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

boot manual

Use the **boot manual** global configuration command 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
	12.1(14)AX	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 <i>switch:</i> 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, “Catalyst 3750 Metro Switch Boot Loader Commands.”

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

boot private-config-file

Use the **boot private-config-file** global configuration command to specify the filename that software 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 <i>private-config</i> .					
Command Modes	Global configuration					
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.1(14)AX</td><td>This command was introduced.</td></tr></table>		Release	Modification	12.1(14)AX	This command was introduced.
Release	Modification					
12.1(14)AX	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 <i>pconfig</i>: <pre>Switch(config)# boot private-config-file pconfig</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show boot</td><td>Displays the settings of the boot environment variables.</td></tr></table>		Command	Description	show boot	Displays the settings of the boot environment variables.
Command	Description					
show boot	Displays the settings of the boot environment variables.					

boot system

Use the **boot system** global configuration command to specify the 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 flash: 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
12.1(14)AX	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, “Catalyst 3750 Metro Switch Boot Loader Commands.”](#)

Related Commands

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

channel-group

Use the **channel-group** interface configuration command to assign a port to an EtherChannel group and to enable an EtherChannel mode. Use the **no** form of this command to remove a 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**

Syntax Description

channel-group-number	Specify the channel group number. The range is 1 to 12.
mode	Specify the EtherChannel mode of the port.
active	Unconditionally enable Link Aggregation Protocol (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.
auto	Enable the Port Aggregation Protocol (PAgP) only if a PAgP device is detected. Auto mode places a port into a passive negotiating state in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation. A channel is formed only with another port group in desirable mode. When auto is enabled, silent operation is the default.
desirable	Unconditionally enable PAgP. Desirable mode places a port into an active negotiating state in which the port starts negotiations with other ports by sending PAgP packets. A channel is formed with another port group in either the desirable or auto mode. When desirable is enabled, silent operation is the default.
non-silent	(Optional) Used with the auto or desirable keyword when traffic is expected from the other device.
on	Enable on mode. In on mode, a usable EtherChannel exists only when both connected port groups are in the on mode.
passive	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
12.1(14)AX	This command was introduced.

Usage Guidelines

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

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

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 apply to all the physical ports assigned to the port-channel. 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, 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.

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

**Caution**

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

**Note**

Enhanced-services (ES) port cannot be bundled with non ES ports.

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

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

Do not configure a port that is an active member of an EtherChannel as an 802.1x port. If 802.1x is enabled on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.

**Note**

If 802.1x is enabled on a not-yet active port of an EtherChannel in software releases earlier than Cisco IOS Release 12.2(25)EY, the port does not join the EtherChannel.

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 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 EtherChannel. It assigns ports as static-access ports in VLAN 10 to channel 5 with the PAgP mode **desirable**.

```
Switch# configure terminal
Switch(config)# interface range fastethernet1/0/4 -5
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 EtherChannel. It assigns ports as static-access ports in VLAN 10 to channel 5 with the LACP mode **active**.

```
Switch# configure terminal
Switch(config)# interface range fastethernet1/0/4 -5
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

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

Related Commands

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

Command	Description
show pagp	Displays PAgP channel-group information.
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 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

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

Defaults

No protocol is assigned to the EtherChannel.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

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

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

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

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

Examples

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

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

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

Related Commands

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

class

Use the **class** policy-map configuration command to specify the name of the class whose traffic policy you want to create or change. Use the **no** form of this command to delete an existing class from a policy map.

class *class-name*

no class *class-name*

Syntax Description

<i>class-name</i>	Name of the predefined traffic class for which you want to configure or modify a traffic policy. The class was previously created through the class-map <i>class-map-name</i> global configuration command.

Defaults

No classes are defined.

Command Modes

Policy-map configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

Before using the **class** command, you must create a class map for matching packets to the class by using the **class-map** global configuration command. You also must 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 traffic policy for new classes or modify a traffic policy for any existing classes in that policy map. The class name that you specify with the **class** command in the policy map ties the characteristics for that class—that is, its policy—to the class map and its match criteria, as configured through the **class-map** global configuration command. You attach the policy map to a port by using the **service-policy** interface configuration command.

After you enter the **class** command, the switch enters policy-map class configuration mode, and these configuration commands are available:

- **bandwidth**: specifies or modifies the minimum bandwidth provided to a class belonging to a policy map. For more information, see the **bandwidth** command. This command is effective only in a hierarchical policy map attached to an enhanced-services (ES) port.
- **exit**: exits policy-map class configuration mode and returns to policy-map configuration mode.
- **no**: returns a command to its default setting.
- **police**: configures a single-rate policer, an aggregate policer, or a two-rate traffic policer that uses the committed information rate (CIR) and the peak information rate (PIR) for a class of 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** commands. For more information about the two-rate policer, see the **police cir** and the **police cir percent** command. The two-rate traffic policer commands are effective only in a hierarchical policy map attached to an ES port.

- **priority**: enables the priority queue (low-latency queueing [LLQ]) for a class of traffic. For more information, see the **priority** command. This command is effective only in a hierarchical policy map attached to an ES port.
- **queue-limit**: configures the maximum packet threshold for tail drop for a class configured in a policy map attached to an ES port. For more information, see the **queue-limit** command. This command is effective only in a hierarchical policy map attached to an ES port.
- **random-detect**: configures Weighted Random Early Detection (WRED) as a drop policy. For more information, see the **random-detect** command. This command is effective only in a hierarchical policy map attached to an ES port.
- **service-policy**: creates a service policy as a quality of service (QoS) policy within a policy map (called a hierarchical service policy). For more information, see the **service-policy (policy-map class)** command. This command is effective only in a hierarchical policy map attached to an ES port.
- **set**: classifies IP traffic by setting a class of service (CoS), a Differentiated Services Code Point (DSCP), an IP-precedence, or the multiprotocol label switching (MPLS) experimental (EXP) bits in the packet. For more information, see the **set** command. Some keywords are effective only in a hierarchical policy map attached to an ES port.
- **shape**: sets the token bucket committed information rate (CIR) in a policy map. For more information, see the **shape** command. This command is effective only in a hierarchical policy map attached to an ES port.
- **trust**: defines a trust state for a traffic class. For more information, see the **trust** command.

The switch supports up to eight classes, including the default class, in a policy map. Packets that fail to meet any of the matching criteria are classified as members of the default traffic class. You configure the default traffic class by specifying **class-default** as the class name in the **class** policy-map class configuration command. You can manipulate the default traffic class (for example, set policies to police or to shape it) just like any other traffic class, but you cannot delete it.

Within a policy map, the class-default applies to all traffic that is not explicitly matched within the policy map but that does match the parent policy. If no parent policy is configured, the parent policy represents the physical port. In the physical-level policy map, class-default is the only class that can be configured.

In a hierarchical policy map attached to an ES port, you define a class policy to use either tail drop or WRED packet drop by using either the **queue-limit** policy-map class configuration command or the **random-detect** policy-map class configuration command, respectively. You cannot use the **queue-limit** and **random-detect** commands in the same class policy, but they can be used in two class policies in the same policy map.

In a hierarchical policy map attached to an ES port, you must configure the **bandwidth** or the **shape** policy-map class configuration command before you configure either the **queue-limit** or the **random-detect** policy-map class configuration command in a class policy.

When you configure a policy for a class, specify its bandwidth, and attach the policy map to an ES port, class-based weighted fair queueing (CBWFQ) determines if the bandwidth requirement of the class can be satisfied. If so, CBWFQ creates the necessary internal data structures to maintain the state for the class and allocates a queue for it. If CBWFQ decides that the bandwidth requirement for the class cannot be satisfied, an error message appears, and the policy is not attached. When a class is removed, available bandwidth for the port is incremented by the amount previously allocated to the class.

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*. When attached to an ingress port, the policy matches all the inbound traffic defined in *class1*, sets the IP DSCP to 10, and polices the traffic at an average rate of 1 Mbps and bursts of 20 KB. Traffic exceeding the profile is marked down to a DSCP value obtained from the policed-DSCP map and then sent.

```
Switch(config)# class-map class1
Switch(config-cmap)# exit
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set ip dscp 10
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet1/0/4
Switch(config-if)# service-policy input policy1
```

This example configures two class policies included in the egress policy map called *policy1*. Class1 specifies a policy for 802.1Q tunneling traffic that matches packets based on the outer VLAN ID (VLAN 2) and the inner VLAN IDs (3 to 8).

```
Switch(config)# class-map match-all class1
Switch(config-cmap)# match vlan 2
Switch(config-cmap)# match vlan inner 3 - 8
Switch(config-cmap)# exit
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# bandwidth 2000
Switch(config-pmap-c)# queue-limit 40
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# service-policy output policy1
```

For class1, a minimum of 2000 kbps of bandwidth is expected to be delivered to this class in the event of congestion. The queue reserved for this class can contain 40 packets before tail drop occurs.

This example shows how to shape the default class. This configuration associates a class-level policy map with a VLAN-level policy map and then associates the VLAN-level policy map with a physical-level policy map.

```
Switch(config)# class-map my-class
Switch(config-cmap)# match ip precedence 1
Switch(config-cmap)# exit
Switch(config)# class-map my-logical-class
Switch(config-cmap)# match vlan 5
Switch(config-cmap)# exit
Switch(config)# policy-map my-class-policy
Switch(config-pmap)# class my-class
Switch(config-pmap-c)# set ip precedence 2
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map my-logical-policy
Switch(config-pmap)# class my-logical-class
Switch(config-pmap-c)# shape average 400000000
Switch(config-pmap-c)# service-policy my-class-policy
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map my-physical-policy
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 500000000
Switch(config-pmap-c)# service-policy my-logical-policy
```

This example shows how to create a hierarchical class-level policy map with two traffic classes. One of the classes has a class-level classification and a two-rate policer, and the other is the default traffic class. Packets that fail to meet the matching criteria are classified as members of the default traffic class, and the IP precedence in this traffic is reset to 0.

```
Switch(config)# class-map match-all classprec1
Switch(config-cmap)# match ip precedence 1
Switch(config-cmap)# exit
Switch(config)# policy-map precedencepolice
Switch(config-pmap)# class classprec1
Switch(config-pmap-c)# police cir 100000000 pir 200000000 conform-action set-prec-transmit
2 exceed-action set-prec-transmit 3 violate-action set-prec-transmit 4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set ip precedence 0
```

In the previous hierarchical QoS example, the first traffic class has only one match statement. However, hierarchical policy maps can support multiple match statements.

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

Related Commands

Command	Description
bandwidth	Specifies or modifies the minimum bandwidth provided to a class belonging to a policy map attached to an ES port.
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
police	Configures a single-rate traffic policer for a class of traffic.
police cir	Configures a two-rate traffic policer for a class of traffic.
police cir percent	Configures a two-rate traffic policer for a class of traffic based on a percentage of the available bandwidth.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
priority	Enables the strict-priority queue and gives priority to a class of traffic belonging to a policy map attached to an ES port.
queue-limit	Configures the maximum threshold for tail drop in a policy map attached to an ES port.
random-detect	Configures WRED in a policy map attached to an ES port.
service-policy (interface configuration)	Applies a policy map defined by the policy-map global configuration command to a port.
service-policy (policy-map class)	Creates a service policy as a QoS policy within a policy map.
set	Classifies IP traffic by setting a CoS, a DSCP, an IP-precedence, or the MPLS EXP bits in the packet.
shape	Enables traffic shaping in a policy map attached to an ES port.
show policy-map	Displays QoS policy maps.
trust	Defines a trust state for the traffic classified through the class policy-map configuration command.

class-map

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

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

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

Syntax Description

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

Defaults

No class maps are defined.

If neither the **match-all** nor the **match-any** keyword is specified, the default is **match-all**.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

Use this command to specify the name of the class for which you want to create or modify class-map match criteria and to enter class-map configuration mode. Packets are checked against the match criteria configured for a class map to decide if the packet belongs to that class. If a packet matches the specified criteria, the packet is considered a member of the class and is forwarded according to the quality of service (QoS) specifications set in the traffic policy.

You can create up to 4093 class maps.

After you enter the **class-map** command, the switch enters class-map configuration mode, and these configuration commands are available:

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

Only one access control list (ACL) can be configured in a class map. The ACL can have multiple access control entries (ACEs). Class maps that contain ACLs are not supported in an egress policy attached to an enhanced-services (ES) port or in a hierarchical ingress policy attached to an ES port.

Examples

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

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

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

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

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

Related Commands

Command	Description
class	Specifies the name of the class whose traffic policy you want to create or change.
match (class-map configuration)	Defines the match criteria for a class map.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show class-map	Displays QoS class maps.

clear ip arp inspection log

Use the **clear ip arp inspection log** privileged EXEC command on the switch stack or on a standalone switch to clear the dynamic Address Resolution Protocol (ARP) inspection log buffer.

clear ip arp inspection log

This command is available only if your switch is running the enhanced multilayer image (EMI).

Syntax Description

This command has no arguments or keywords.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)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
arp access-list	Defines an ARP access control list (ACL).
ip arp inspection log-buffer	Configures the dynamic ARP inspection logging buffer.
ip arp inspection vlan logging	Controls the type of packets that are logged per VLAN.
show ip arp inspection log	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 on the switch stack or on a standalone switch to clear the dynamic Address Resolution Protocol (ARP) inspection statistics.

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

This command is available only if your switch is running the enhanced multilayer image (EMI).

Syntax Description

vlan <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.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)EY	This command was introduced.

Examples

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.

Related Commands

Command	Description
show ip arp inspection statistics	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 snooping binding database, the DHCP snooping 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

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

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)EY	This command was introduced.
12.2(37)SE	The statistics keyword was introduced.
12.2(44)SE	The * , ip-address , interface <i>interface-id</i> , and vlan <i>vlan-id</i> keywords were 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:

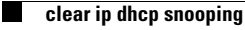
```
Switch# clear ip dhcp snooping database statistics
```

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
	ip dhcp snooping	Enables DHCP snooping on a VLAN.
	ip dhcp snooping database	Configures the DHCP snooping binding database agent or the binding file.
	show ip dhcp snooping binding	Displays the status of DHCP snooping database agent.
	show ip dhcp snooping database	Displays the DHCP snooping binding database agent statistics.
	show ip dhcp snooping statistics	Displays the DHCP snooping statistics.

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*]

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

Defaults	No default is defined.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	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 a port:
	Switch # clear l2protocol-tunnel counters gigabitethernet1/0/2
You can verify that the information was deleted by entering the show l2protocol-tunnel privileged EXEC command.	

Related Commands	Command	Description
	show l2protocol-tunnel	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** }

Syntax Description

<i>channel-group-number</i>	(Optional) Channel group number. The range is 1 to 12.
counters	Clear traffic counters.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

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

Examples

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

```
Switch# clear lacp counters
```

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

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

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

Related Commands

Command	Description
show lacp	Displays LACP channel-group information.

clear mac address-table

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

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

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

Defaults No default is defined.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	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
	mac address-table notification	Enables the MAC address notification feature.
	show mac address-table	Displays the MAC address table static and dynamic entries.
	show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
	snmp trap mac-notification	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

Syntax Description This command has no arguments or keywords.

Defaults No default is defined.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(25)SED	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
	mac address-table move update	Configures MAC address-table move update on the switch.
	show mac address-table move update	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**}

Syntax Description

<i>channel-group-number</i>	(Optional) Channel group number. The range is 1 to 12.
counters	Clear traffic counters.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

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

Examples

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

```
Switch# clear pagp counters
```

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

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

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

Related Commands

Command	Description
show pagp	Displays PAgP channel-group information.

clear 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*]

Syntax Description	interface <i>interface-id</i> (Optional) Specify a REP interface whose counters should be cleared.	
Defaults	No default is defined.	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	122(46)SE	This command was introduced.
Usage Guidelines	You can clear all REP counters by using the clear rep counters command, or you can clear only the counters for the interface by using the clear rep counters interface <i>interface-id</i> command. When you enter the clear rep counters command, only the counters visible in the output of the show interface rep detail command are cleared. SNMP visible counters are not cleared as they are read-only.	
Examples	This example shows how to clear all REP counters for all REP interfaces: <pre>Switch# clear rep counters</pre> You can verify that REP information was deleted by entering the show interfaces rep detail privileged EXEC command.	
Related Commands	Command	Description
	show interfaces rep detail	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*]

Syntax Description	interface <i>interface-id</i> (Optional) Clear all spanning-tree counters on the specified interface. Valid interfaces include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 12.

Defaults	No default is defined.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

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

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

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

clear spanning-tree detected-protocols

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

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

Syntax Description	interface <i>interface-id</i> (Optional) Restart the protocol migration process on the specified interface. Valid interfaces include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 12.

Defaults	No default is defined.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	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 802.1D switches. If a rapid-PVST+ switch or an MSTP switch receives a legacy 802.1D configuration bridge protocol data unit (BPDU) with the protocol version set to 0, it sends only 802.1D BPDUs on that interface. A multiple spanning-tree (MST) switch can also detect that an interface 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 802.1D BPDUs. It cannot detect 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: <pre>Switch# clear spanning-tree detected-protocols interface gigabitethernet1/0/1</pre>

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

clear vmps statistics

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

clear vmps statistics

Syntax Description	This command has no arguments or keywords.

Defaults	No default is defined.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

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

Switch# **clear vmps statistics**

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

Related Commands	Command	Description
	show vmps	Displays the VQP version, reconfirmation interval, retry count, VMPS IP addresses, and the current and primary servers.

clear vtp counters

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

clear vtp counters

Syntax Description This command has no arguments or keywords.

Defaults No default is defined.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Examples This example shows how to clear the VTP counters:

```
Switch# clear vtp counters
```

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

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

cluster commander-address

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

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

no cluster commander-address

Syntax Description

<i>mac-address</i>	MAC address of the cluster command switch.
member <i>number</i>	(Optional) Number of a configured cluster member switch. The range is 0 to 15.
name <i>name</i>	(Optional) Name of the configured cluster up to 31 characters.
vlan <i>vlan-id</i>	(Optional) VLAN to communicate with the command switch. The range is 1 to 4094.

Defaults

The switch is not a member of any cluster.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

This command is available only on the cluster command switch.

A cluster member can have only one cluster command switch.

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

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

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

Examples

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

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

<output truncated>

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

<output truncated>

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

Switch # **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)# **no cluster commander-address**

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

Related Commands

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

cluster discovery hop-count

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

cluster discovery hop-count *number*

no cluster discovery hop-count

Syntax Description	<i>number</i>	Number of hops from the cluster edge that the cluster command switch limits the discovery of candidates. The range is 1 to 7.

Defaults	The hop count is set to 3.

Command Modes	Global configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	This command is available only on the cluster command switch. This command does not operate on cluster member switches.
	If the hop count is set to 1, it disables extended discovery. The cluster command switch discovers only candidates that are one hop from the edge of the cluster. The edge of the cluster is the point between the last discovered cluster member switch and the first discovered candidate switch.

Examples	This example shows how to set hop count limit to 4. This command is executed on the cluster command switch.
	Switch(config)# cluster discovery hop-count 4

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

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

cluster enable

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

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

no cluster enable

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

Defaults

The switch is not a cluster command switch.

No cluster name is defined.

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

Command Modes

Global configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

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

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

cluster holdtime

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

cluster holdtime *holdtime-in-secs*

no cluster holdtime

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

Defaults	The default holdtime is 80 seconds.

Command Modes	Global configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

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

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

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

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

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

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

cluster member

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

cluster member [*n*] **mac-address** *H.H.H* [**password** *enable-password*] [**vlan** *vlan-id*]

no cluster member *n*

Syntax Description

<i>n</i>	The number that identifies a cluster member. The range is 0 to 15.
mac-address <i>H.H.H</i>	MAC address of the cluster member switch in hexadecimal format.
password <i>enable-password</i>	Enable password of the candidate switch. The password is not required if there is no password on the candidate switch.
vlan <i>vlan-id</i>	(Optional) VLAN ID through which the candidate is added to the cluster by the cluster command switch. The range is 1 to 4094.

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

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

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

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

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

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

Examples

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

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

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

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

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

Related Commands

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

cluster outside-interface

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

cluster outside-interface *interface-id*

no cluster outside-interface

Syntax Description

<i>interface-id</i>	Interface to serve as the outside interface. Valid interfaces include physical interfaces, port-channels, or VLANs. The port-channel range is 1 to 12. The VLAN range is 1 to 4094.

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

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

Examples

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

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

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

Related Commands

Command	Description
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.

cluster run

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

cluster run

no cluster run

Syntax Description	This command has no arguments or keywords.

Defaults	Clustering is enabled on all switches.

Command Modes	Global configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	When you enter the no cluster run command on a cluster command switch, the cluster command switch is disabled. Clustering is disabled, and the switch cannot become a candidate switch.
	When you enter the no cluster run command on a cluster member switch, it is removed from the cluster. Clustering is disabled, and the switch cannot become a candidate switch.
	When you enter the no cluster run command on a switch that is not part of a cluster, clustering is disabled on this switch. This switch cannot then become a candidate switch.

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

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

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

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

cluster standby-group

Use the **cluster standby-group** global configuration command to enable cluster command-switch redundancy by binding the cluster to an existing Hot Standby Router Protocol (HSRP). Entering the routing-redundancy keyword enables the same HSRP group to be used for cluster command-switch redundancy and routing redundancy. Use the **no** form of this command to return to the default setting.

cluster standby-group *HSRP-group-name* [**routing-redundancy**]

no cluster standby-group

Syntax Description	<i>HSRP-group-name</i>	Name of the HSRP group that is bound to the cluster. The group name is limited to 32 characters.
	routing-redundancy	(Optional) Enable the same HSRP standby group to be used for cluster command-switch redundancy and routing redundancy.

Defaults The cluster is not bound to any HSRP group.

Command Modes Global configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines

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

The cluster command switch propagates the cluster-HSRP binding information to all cluster-HSRP capable members. Each cluster member switch stores the binding information in its NVRAM.

The HSRP group name must be a valid standby group; otherwise, the command exits with an error.

The same group name should be used on all members of the HSRP standby group that is to be bound to the cluster. The same HSRP group name should also be used on all cluster-HSRP capable members for the HSRP group that is to be bound. (When not binding a cluster to an HSRP group, you can use different names on the cluster commander and the members.)

Examples This example shows how to bind the HSRP group named *my_hsrp* to the cluster. This command is executed on the cluster command switch.

```
Switch(config)# cluster standby-group my_hsrp
```

This example shows how to use the same HSRP group named *my_hsrp* for routing redundancy and cluster redundancy:

```
Switch(config)# cluster standby-group my_hsrp routing-redundancy
```

■ cluster standby-group

This example shows the error message when this command is executed on a cluster command switch and the specified HSRP standby group does not exist:

```
Switch(config)# cluster standby-group my_hsrp
%ERROR: Standby (my_hsrp) group does not exist
```

This example shows the error message when this command is executed on a cluster member switch:

```
Switch(config)# cluster standby-group my_hsrp routing-redundancy
%ERROR: This command runs on a cluster command switch
```

You can verify your settings by entering the **show cluster** privileged EXEC command. The output shows whether redundancy is enabled in the cluster.

Related Commands	Command	Description
	standby ip	Enables HSRP on the interface. For syntax information, select Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands .
	show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.
	show standby	Displays standby group information. For syntax information, select Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands .

cluster timer

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

cluster timer *interval-in-secs*

no cluster timer

Syntax Description	<i>interval-in-secs</i>	Interval in seconds between heartbeat messages. The range is 1 to 300 seconds.

Defaults	The interval is 8 seconds.

Command Modes	Global configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	Enter this command with the cluster holdtime global configuration command only on the cluster command switch. The cluster command switch propagates the values to all its cluster members so that the setting is consistent among all switches in the cluster. The holdtime is typically set as a multiple of the heartbeat interval timer (cluster timer). For example, it takes (holdtime-in-secs divided by the interval-in-secs) number of heartbeat messages to be missed in a row to declare a switch down.

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

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

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

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

cpu traffic qos

Use the **cpu traffic qos** global configuration command to configure quality of service (QoS) packet marking for CPU-generated traffic. Use the **no** form of this command to return to the default setting.

cpu traffic qos [*cos value* | *dscp value* | *precedence value*]

no cpu traffic qos [*cos value* | *dscp value* | *precedence value*]

Syntax Description	<i>cos value</i>	(Optional) Set the class of service (CoS) value. The range is from 0 to 7.
	<i>dscp value</i>	(Optional) Set the Differentiated Services Code Point (DSCP) value. The range is from 0 to 63. You also can enter a mnemonic name for a commonly used value.
	<i>precedence value</i>	(Optional) Set the parameters for each IP precedence value. The range is from 0 to 7. You also can enter a mnemonic name for a commonly used value.

Defaults	The default egress queue value is 2. However, if there is no output policy attached to the port, the CPU-generated traffic is sent through the first non-priority queue defined in the output policy map.

Command Modes	Global configuration

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

Usage Guidelines	Use the cpu traffic qos global configuration command to mark the control plane traffic that the CPU generates.
	You must globally enable mls qos global configuration command on the switch to use the cpu traffic qos feature.
	When you mark CPU-generated traffic with CoS, DSCP, or IP precedence values, the control protocol traffic is marked with these values, except for Connectivity Fault Management (CFM) traffic and Cisco IOS IP Service Level Agreements (SLAs). Any changes that you make using the cpu traffic qos global configuration command does not affect the CFM traffic or IP SLA CoS markings.

Examples	This example shows how to configure the DSCP marking value to af11 for CPU-generated traffic:
	Switch(config)# cpu traffic qos dscp af11
	You can verify your settings by entering the show cpu traffic qos privileged EXEC command.

Related Commands

Command	Description
show cpu traffic qos	Displays the QoS output for CPU-generated traffic.
mls qos srr-queue output cpu-queue	Maps all traffic that the CPU generates to an output queue and a threshold ID.

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*

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
12.1(14)AX	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, **fastethernet1/0/1 -5** is a valid range; **fastethernet1/0/1-5** 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 12
- **fastethernet** switch number (always 1)/module/{*first port*} - {*last port*}
- **gigabitethernet** switch number (always 1)/module/{*first port*} - {*last port*}

For physical interfaces:

- switch number is always 1.

- module number is 0 for 10/100 ports and standard SFP module slots; 1 for enhanced-services (ES) ports.
- the range is *type 1/module-number/number - number* (for example, **gigabitethernet 1/0/1 - 2**)

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

gigabitethernet1/0/1 - 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:

fastethernet1/0/3 , gigabitethernet1/0/1 - 2

fastethernet1/0/3 -4 , gigabitethernet1/0/1 - 2

Examples

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

```
Switch(config)# define interface-range macro1 fastethernet1/0/1 -2 , fastethernet1/0/5
```

Related Commands

Command	Description
interface range	Executes a command on multiple ports at the same time.
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 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	/force	(Optional) Suppress the prompt that confirms the deletion.
	/recursive	(Optional) Delete the named directory and all subdirectories and the files contained in it.
	filesystem:	Alias for a flash file system. The syntax for the local flash file system: flash:
	/file-url	The path (directory) and filename to delete.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	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 <i>Cisco IOS Command Reference for Release 12.2</i> .

Examples	This example shows how to remove the directory that contains the old software image after a successful download of a new image:
	Switch# delete /force /recursive flash:/old-image
	You can verify that the directory was removed by entering the dir filesystem: privileged EXEC command.

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

deny

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 | lavc-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 | lavc-sca | lsap lsap mask | mop-console |
mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp]
```

Syntax	Description
any	Keyword to specify to deny any source or destination MAC address.
host <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.
host <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.
aarp	(Optional) Select Ethertype AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
amber	(Optional) Select EtherType DEC-Amber.
cos <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 cos option is configured.
dec-spanning	(Optional) Select EtherType Digital Equipment Corporation (DEC) spanning tree.
decnet-iv	(Optional) Select EtherType DECnet Phase IV protocol.
diagnostic	(Optional) Select EtherType DEC-Diagnostic.
dsm	(Optional) Select EtherType DEC-DSM.
etype-6000	(Optional) Select EtherType 0x6000.
etype-8042	(Optional) Select EtherType 0x8042.
lat	(Optional) Select EtherType DEC-LAT.
lavc-sca	(Optional) Select EtherType DEC-LAVC-SCA.

deny

lsap <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. <i>mask</i> is a mask of <i>don't care</i> bits applied to the LSAP number before testing for a match.
mop-console	(Optional) Select EtherType DEC-MOP Remote Console.
mop-dump	(Optional) Select EtherType DEC-MOP Dump.
msdos	(Optional) Select EtherType DEC-MSDOS.
mumps	(Optional) Select EtherType DEC-MUMPS.
netbios	(Optional) Select EtherType DEC- Network Basic Input/Output System (NETBIOS).
vines-echo	(Optional) Select EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
vines-ip	(Optional) Select EtherType VINES IP.
xns-idp	(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 2-4](#).

Table 2-4 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
12.1(14)AX	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
mac access-list extended	Creates an access list based on MAC addresses for non-IP traffic.
permit	Permits non-IP traffic to be forwarded if conditions are matched.
show access-lists	Displays access control lists configured on a switch.

deny (ARP access-list configuration)

Use the **deny** Address Resolution Protocol (ARP) access-list configuration command on the switch stack or on a standalone switch 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]
```

This command is available only if your switch is running the enhanced multilayer image (EMI).

Syntax Description

request	(Optional) Define a match for the ARP request. When request is not specified, matching is performed against all ARP packets.
ip	Specify the sender IP address.
any	Deny any IP or MAC address.
host <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.
mac	Deny the sender MAC address.
host <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.
response ip	Define the IP address values for the ARP responses.
host <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.
mac	Deny the MAC address values for the ARP responses.
host <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.
log	(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(25)EY	This command was introduced.

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

dot1x auth-fail max-attempts

Use the **dot1x auth-fail max-attempts** interface configuration command to configure the maximum allowable authentication attempts before a port is moved to the restricted VLAN. To return to the default setting, use the **no** form of this command.

dot1x auth-fail max-attempts *max-attempts*

no dot1x auth-fail max-attempts

Syntax Description	<i>max-attempts</i>	Specify a maximum number of authentication attempts allowed before a port is moved to the restricted VLAN. The range is 1 to 3, the default value is 3.

Defaults	The default value is 3 attempts.

Command Modes	Interface configuration

Command History	Release	Modification
	12.2(25)SED	This command was introduced.

Usage Guidelines	If you reconfigure the maximum number of authentication attempts allowed by the VLAN, the change takes effect after the re-authentication timer expires.

Examples	This example shows how to set 2 as the maximum number of authentication attempts allowed before the port is moved to the restricted VLAN on port 3: <pre>Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# interface gigabitethernet1/0/3 Switch(config-if)# dot1x auth-fail max-attempts 2 Switch(config-if)# end Switch(config)# end Switch#</pre>
	You can verify your settings by entering the show dot1x [interface interface-id] privileged EXEC command.

Related Commands

Command	Description
dot1x auth-fail vlan [<i>vlan id</i>]	Enables the optional restricted VLAN feature.
dot1x max-reauth-req [<i>count</i>]	Sets the maximum number of times that the switch restarts the authentication process before a port changes to the unauthorized state.
show dot1x [interface <i>interface-id</i>]	Displays IEEE 802.1x status for the specified port.

dot1x auth-fail vlan

Use the **dot1x auth-fail vlan** interface configuration command to enable the restricted VLAN on a port. To return to the default setting, use the **no** form of this command.

dot1x auth-fail vlan *vlan-id*

no dot1x auth-fail vlan *vlan-id*

Syntax Description

<i>vlan-id</i>	Specify a VLAN in the range of 1 to 4094.

Defaults

No restricted VLAN is configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(25)SED	This command was introduced.

Usage Guidelines

You can configure a restricted VLAN on ports configured as follows:

- single-host (default) mode
- auto mode for authorization

You should enable re-authentication. The ports in restricted VLANs do not receive re-authentication requests if it is disabled. To start the re-authentication process, the restricted VLAN must receive a link-down event or an Extensible Authentication Protocol (EAP) logoff event from the port. If a host is connected through a hub, the port might never receive a link-down event when that host is disconnected, and, as a result, might not detect any new hosts until the next re-authentication attempt occurs.

If the supplicant fails authentication, the port is moved to a restricted VLAN, and an EAP *success* message is sent to the supplicant. Because the supplicant is not notified of the actual authentication failure, there might be confusion about this restricted network access. An EAP success message is sent for these reasons:

- If the EAP success message is not sent, the supplicant tries to authenticate every 60 seconds (the default) by sending an EAP-start message.
- Some hosts (for example, devices running Windows XP) cannot implement DHCP until they receive an EAP success message.

A supplicant might cache an incorrect username and password combination after receiving an EAP success message from the authenticator and re-use that information in every re-authentication. Until the supplicant sends the correct username and password combination, the port remains in the restricted VLAN.

Internal VLANs used for Layer 3 ports cannot be configured as restricted VLANs.

You cannot configure a VLAN to be both a restricted VLAN and a voice VLAN. If you do this, a syslog message is generated.

When a restricted VLAN port is moved to an unauthorized state, the authentication process restarts. If the supplicant fails the authentication process again, the authenticator waits in the held state. After the supplicant has correctly re-authenticated, all IEEE 802.1x ports are reinitialized and treated as normal IEEE 802.1x ports.

When you reconfigure a restricted VLAN as a different VLAN, any ports in the restricted VLAN are also moved, and the ports stay in their currently authorized state.

When you shut down or remove a restricted VLAN from the VLAN database, any ports in the restricted VLAN are immediately moved to an unauthorized state, and the authentication process restarts. The authenticator does not wait in a held state because the restricted VLAN configuration still exists. While the restricted VLAN is inactive, all authentication attempts are counted so that when the restricted VLAN becomes active, the port is immediately placed in the restricted VLAN.

The restricted VLAN is supported only in single host mode (the default port mode). For this reason, when a port is placed in a restricted VLAN, the supplicant's MAC address is added to the MAC address table, and any other MAC address that appears on the port is treated as a security violation.

Examples

This example shows how to configure a restricted VLAN on port 1:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# dot1x auth-fail vlan 40
Switch(config-if)# end
Switch(config)# end
Switch#
```

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

Related Commands

Command	Description
dot1x auth-fail max-attempts [<i>max-attempts</i>]	Configures the number of authentication attempts allowed before assigning a supplicant to the restricted VLAN.
show dot1x [interface interface-id]	Displays IEEE 802.1x status for the specified port.

dot1x default

Use the **dot1x default** interface configuration command to reset the configurable 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 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
12.1(14)AX	This command was introduced.

Examples

This example shows how to reset the configurable 802.1x parameters:

```
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
show dot1x [interface interface-id]	Displays 802.1x status for the specified port.

dot1x guest-vlan

Use the **dot1x guest-vlan** interface configuration command to specify an active VLAN as an 802.1x guest VLAN. Use the **no** form of this command to return to the default setting.

dot1x guest-vlan *vlan-id*

no dot1x guest-vlan

Syntax Description	<i>vlan-id</i>	Specify an active VLAN as an 802.1x guest VLAN. The range is 1 to 4094.

Defaults	No guest VLAN is configured.

Command Modes	Interface configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	When you configure a guest VLAN, clients that are not 802.1x-capable are put into the guest VLAN when the server does not receive a response to its Extensible Authentication Protocol over LAN (EAPOL) request/identity frame. Clients that are 802.1x-capable but fail authentication are not granted access to the network.

Guest VLANs are supported on 802.1x ports in single-host mode and multiple-hosts mode.

The switch maintains the EAPOL packet history. If another EAPOL packet is detected on the interface during the lifetime of the link, the guest VLAN feature is disabled. If the port is already in the guest VLAN state, the port is returned to the unauthorized state, and authentication is restarted. The EAPOL history is reset upon loss of link.

Entering the **dot1x guest-vlan supplicant** global configuration command disables this behavior.

Any number of non-IEEE 802.1x-capable clients are allowed access when the switch port is moved to the guest VLAN. If an IEEE 802.1x-capable client joins the same port on which the guest VLAN is configured, the port is put into the unauthorized state in the user-configured access VLAN, and authentication is restarted.

Guest VLANs are supported on IEEE 802.1x ports in single-host or multiple-hosts mode.

You can configure any active VLAN except an RSPAN VLAN or a voice VLAN as an 802.1x guest VLAN. The guest VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.

Examples	This example shows how to specify VLAN 5 as an 802.1x guest VLAN:

```
Switch(config-if)# dot1x guest-vlan 5
```

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

Related Commands

Command	Description
show dot1x [interface <i>interface-id</i>]	Displays 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 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]

Syntax Description

multi-host	Enable multiple-hosts mode on the switch.
single-host	Enable single-host mode on the switch.



Note

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

Command Default

The default is single-host mode.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

Use this command to limit an 802.1x-enabled port to a single client or to attach multiple clients to an 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 802.1x globally, enable 802.1x on a port, and enable multiple-hosts mode:

```
Switch(config)# dot1x system-auth-control
Switch(config)# interface gigabitethernet1/0/1
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

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

dot1x initialize

Use the **dot1x initialize** privileged EXEC command to manually return the specified 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 <i>interface-id</i>	Port to be initialized.

Defaults

There is no default setting.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

Use this command to initialize the 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 gigabitethernet1/0/2
```

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

Related Commands

Command	Description
show dot1x [interface interface-id]	Displays 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>	Number of times that the switch restarts the authentication process before the port transitions to the unauthorized state. The range is 1 to 10.

Defaults

The default is 2 times.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(25)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
dot1x max-req	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.
dot1x test eapol-capable tx-period	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.
show dot1x [interface interface-id]	Displays 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 retransmits 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 retransmits an EAP frame from the authentication server before restarting the authentication process. The range is 1 to 10.

Defaults	The default is 2 times.

Command Modes	Interface configuration

Command History	Release	Modification
	12.1(14)AX	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 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
	dot1x test eapol-capable tx-period	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.
	show dot1x [interface interface-id]	Displays 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	Enable 802.1x authentication on the port and cause the port to transition to the authorized or unauthorized state based on the 802.1x authentication exchange between the switch and the client.
	force-authorized	Disable 802.1x authentication on the port and cause the port to transition to the authorized state without any authentication exchange required. The port sends and receives normal traffic without 802.1x-based authentication of the client.
	force-unauthorized	Deny all access through this port by forcing the port to transition 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
	12.1(14)AX	This command was introduced.

Usage Guidelines

You must globally enable 802.1x on the switch by using the **dot1x system-auth-control** global configuration command before enabling 802.1x on a specific port.

The 802.1x protocol is supported on Layer 2 static-access ports, voice VLAN 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 802.1x on a trunk port, an error message appears, and 802.1x is not enabled. If you try to change the mode of an 802.1x-enabled port to trunk, an error message appears, and the port mode is not changed.
- Dynamic ports—A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable 802.1x on a dynamic port, an error message appears, and 802.1x is not enabled. If you try to change the mode of an 802.1x-enabled port to dynamic, an error message appears, and the port mode is not changed.
- Dynamic-access ports—If you try to enable 802.1x on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and 802.1x is not enabled. If you try to change an 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.

- EtherChannel port—Before enabling 802.1x on the port, you must first remove it from the EtherChannel. If you try to enable 802.1x on an EtherChannel or on an active port in an EtherChannel, an error message appears, and 802.1x is not enabled. If you enable 802.1x on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.
- Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) destination ports—You can enable 802.1x on a port that is a SPAN or RSPAN destination port. However, 802.1x is disabled until the port is removed as a SPAN or RSPAN destination. You can enable 802.1x on a SPAN or RSPAN source port.

To globally disable 802.1x on the switch, use the **no dot1x system-auth-control** global configuration command. To disable 802.1x on a specific port, use the **no dot1x port-control** interface configuration command.

Examples

This example shows how to enable 802.1x on a port:

```
Switch(config)# interface fastethernet1/0/1  
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
show dot1x [interface interface-id]	Displays 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 802.1x-enabled port.

dot1x re-authenticate interface *interface-id*

Syntax Description	interface <i>interface-id</i> Port to re-authenticate.

Defaults	There is no default setting.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	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.

Examples	This example shows how to manually re-authenticate the device connected to a port: <pre>Switch# dot1x re-authenticate interface fastethernet1/0/1</pre>

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
	12.1(14)AX	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
	dot1x test eapol-capable reauth-period	Sets the number of seconds between re-authentication attempts.
	show dot1x [interface interface-id]	Displays 802.1x status for the specified port.

dot1x system-auth-control

Use the **dot1x system-auth-control** global configuration command to globally enable 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	802.1x is disabled.

Command Modes	Global configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	You must enable authentication, authorization, and accounting (AAA) and specify the authentication method list before globally enabling 802.1x. A method list describes the sequence and authentication methods to be queried to authenticate a user.

Examples	This example shows how to globally enable 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
	dot1x port-control	Enables manual control of the authorization state of the port.
	show dot1x [interface interface-id]	Displays 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*]

Syntax Description	interface interface-id (Optional) Port to be queried.

Defaults	There is no default setting.

Command Modes	Privileged EXEC

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

Usage Guidelines	Use this command to test the IEEE 802.1x capability of the devices connected to all ports or to specific ports on a switch. There is not a no form of this command.

Examples	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: <pre>switch# dot1x test eapol-capable interface gigabitethernet1/0/13</pre> DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL capable

Related Commands	Command	Description
	dot1x test timeout <i>timeout</i>	Configures the timeout used to wait for EAPOL response to an IEEE 802.1x readiness query.

dot1x test timeout

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*

Syntax Description	<i>timeout</i>	Time in seconds to wait for an EAPOL response. The range is from 1 to 65535 seconds.

Defaults	The default setting is 10 seconds.

Command Modes	Global configuration

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

Usage Guidelines	Use this command to configure the timeout used to wait for EAPOL response. There is not a no form of this command.

Examples	This example shows how to configure the switch to wait 27 seconds for an EAPOL response: Switch# dot1x test timeout 27 You can verify the timeout configuration status by entering the show run privileged EXEC command.

Related Commands	Command	Description
	dot1x test eapol-capable [interface interface-id]	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 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

quiet-period <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.
reauth-period <i>seconds</i>	Number of seconds between re-authentication attempts. The range is 1 to 65535.
server-timeout <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 30 to 65535.
supp-timeout <i>seconds</i>	Number of seconds that the switch waits for the retransmission of packets by the switch to the 802.1x client. The range is 30 to 65535.
tx-period <i>seconds</i>	Number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending 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
12.1(14)AX	This command was introduced.
12.2(40)SE	The range for tx-period seconds is incorrect. The correct range is from 1 to 65535.

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 smaller number 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 25 seconds as the switch-to-authentication server retransmission time:

```
Switch(config)# dot1x timeout server-timeout 25
```

This example shows how to set 25 seconds as the switch-to-client retransmission time for the EAP request frame:

```
Switch(config-if)# dot1x timeout supp-timeout 25
```

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 resending 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
dot1x max-req	Sets the maximum number of times that the switch sends an EAP-request/identity frame before restarting the authentication process.
dot1x reauthentication	Enables periodic re-authentication of the client.
show dot1x	Displays 802.1x status for all ports.

dot1x violation-mode

Use the **dot1x violation-mode** interface configuration command on the switch stack or on a standalone switch 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.
restrict	Generates a syslog error when a violation error occurs.
protect	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(46)SE	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
	<code>show dot1x [interface <i>interface-id</i>]</code>	Displays IEEE 802.1x status for the specified port.

duplex

Use the **duplex** interface configuration command to specify the duplex mode of operation for Fast Ethernet and Gigabit Ethernet ports. Use the **no** form of this command to return the port to its default value.

duplex { auto | full | half }

no duplex

Syntax Description

auto	Enable automatic duplex configuration; port automatically detects whether it should run in full- or half-duplex mode, depending on the attached device mode.
full	Enable full-duplex mode.
half	Enable half-duplex mode (for Fast Ethernet ports only).

Defaults

The default is **auto** for Fast Ethernet ports and for 1000BASE-T small form-factor pluggable (SFP) modules.

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

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.
12.2(25)EY	Support for the half keyword was added for the 100BASE-FX SFP module.

Usage Guidelines

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

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

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

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

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

For 10/100 Mbps ports, if both speed and duplex are set to specific values, the link operates at the negotiated speed and duplex value.

For 10/100/1000 Mbps ports, if both the speed and duplex are set to specific values, autonegotiation is disabled.

Beginning with Cisco IOS Release 12.2(25)EY, you can configure the duplex setting when the speed is set to **auto**.

This command is not available on SFP module ports unless a 1000BASE-T SFP module or a 100BASE-FX MMF SFP module is in the port. All other SFP modules operate only in full-duplex mode.

- When a 1000BASE-T SFP module is in the SFP module port, you can configure duplex mode to **auto** or **full**.
- When a 100BASE-FX SFP module is in the SFP module port, 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 SFP module does not support autonegotiation.

**Note**

The 100BASE-FX SFP modules are not supported on the ES ports.

**Caution**

Changing the interface speed and duplex mode configuration might shut down and reenables the interface during the reconfiguration.

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

Examples

This example shows how to configure a port for full duplex operation:

```
Switch(config)# interface fastethernet1/0/11
Switch(config-if)# duplex full
```

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

Related Commands

Command	Description
show interfaces	Displays the interface settings on the switch.
speed	Sets the speed on a 10/100 or 10/100/1000 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** | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **loopback** | **pagp-flap** }

no errdisable detect cause { **all** | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **loopback** | **pagp-flap** }

Syntax Description

all	Enable error detection for all error-disabled causes.
dtp-flap	Enable error detection for the Dynamic Trunking Protocol (DTP) flapping.
gbic-invalid	Enable error detection for an invalid GBIC. This error refers to an invalid small form-factor pluggable (SFP) module interface cause.
l2ptguard	Enable error detection for a Layer 2 protocol-tunnel error-disabled cause.
link-flap	Enable error detection for link-state flapping.
loopback	Enable error detection for detected loopbacks.
pagp-flap	Enable error detection for the Port Aggregation Protocol (PAgP) flap-error-disabled cause.



Note

Though visible in the command-line help strings, the **dhcp-rate-limit** keyword is not supported.

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
12.1(14)AX	This command was introduced.

Usage Guidelines

A cause (**dtp-flap**, **gbic-invalid**, **l2ptguard**, **link-flap**, **loopback**, and **pagp-flap**) 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 link-down state.

When a port is error-disabled, it is effectively shut down, and no traffic is sent or received on the 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
show errdisable detect	Displays errdisable detection information.
show interfaces status err-disabled	Displays interface status or a list of interfaces in the error-disabled state.

errdisable detect cause small-frame

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

errdisable detect cause small-frame

no errdisable detect cause small-frame

Syntax Description	This command has no arguments or keywords.

Defaults	This feature is disabled.

Command Modes	Global configuration

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

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

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

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

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

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

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

errdisable recovery cause small-frame

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

errdisable recovery cause small-frame

no errdisable recovery cause small-frame

Syntax Description This command has no arguments or keywords.

Defaults This feature is disabled.

Command Modes Global configuration

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

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

Examples This example shows how to set the recovery timer:

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

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

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

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 | dtp-flap |
gbic-invalid | l2ptguard | link-flap | loopback | pagp-flap | psecure-violation |
security-violation | udld | vmps} | {interval interval}}
```

```
no errdisable recovery {cause {all | arp-inspection | bpduguard | channel-misconfig | dtp-flap |
gbic-invalid | l2ptguard | link-flap | loopback | pagp-flap | psecure-violation |
security-violation | udld | vmps} | {interval interval}}
```

Syntax Description

cause	Enable error disable to recover from a specific cause.
all	Enable the timer to recover from all error-disable causes.
arp-inspection	Enable error detection for dynamic Address Resolution Protocol (ARP) inspection.
bpduguard	Enable the timer to recover from the bridge protocol data unit (BPDU) guard error-disable state.
channel-misconfig	Enable the timer to recover from the EtherChannel misconfiguration error-disable state.
dtp-flap	Enable the timer to recover from the Dynamic Trunking Protocol (DTP) flap error-disable state.
gbic-invalid	Enable the timer to recover from an invalid GBIC error-disable state. This error refers to an invalid small form-factor pluggable (SFP) interface state.
l2ptguard	Enable the timer to recover from a Layer 2 protocol tunnel error-disable state.
link-flap	Enable the timer to recover from the link-flap error-disable state.
loopback	Enable the timer to recover from a loopback error-disable state.
pagp-flap	Enable the timer to recover from the Port Aggregation Protocol (PAgP)-flap error-disable state.
psecure-violation	Enable the timer to recover from a port security violation disable state.
security-violation	Enable the timer to recover from an 802.1x-violation disable state
udld	Enable the timer to recover from the UniDirectional Link Detection (UDLD) error-disabled state.
vmps	Enable the timer to recover from the VLAN Membership Policy Server (VMPS) error-disabled state.
interval interval	Specify the time to recover from the specified error-disabled state. The range is 30 to 86400 seconds. The same interval is applied to all causes. The default interval is 300 seconds.
Note	The error-disabled recovery timer is initialized at a random differential from the configured interval value. The difference between the actual timeout value and the configured value can be up to 15 percent of the configured interval.

**Note**

Though visible in the command-line help strings, the **dhcp-rate-limit**, **unicast-flood**, and **channel-misconfig** keywords are not supported.

Defaults

Recovery is disabled for all causes.
The default recovery interval is 300 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.
12.2(25)EY	The arp-inspection keyword was added.

Usage Guidelines

A cause (**bpduguard**, **dtp-flap**, **gbic-invalid**, **l2ptguard**, **link-flap**, **loopback**, **pagp-flap**, **psecure-violation**, **security-violation**, **udld**, **vmpps**) is defined as the reason why 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-disable cause:

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

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

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

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

Related Commands

Command	Description
show etherchannel	Displays errdisable recovery timer information.
show interfaces status err-disabled	Displays interface status or a list of interfaces in error-disabled state.

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	evc-id	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(25)SEG	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-evc)#

Related Commands	Command	Description
	service instance id ethernet evc-id	Configures an Ethernet service instance and attaches an EVC to it.
	show ethernet service evc	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

ce	Enable the switch as an E-LMI CE device.
Note	Ethernet LMI is disabled by default. You must enable it globally or on an interface in addition to enabling it in CE mode.
global	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(25)SEG	This command was introduced.
12.2(37)SE	The ce keyword was added.

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** interface configuration command, go to this URL: http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a0080690f2d.html#wp1166797

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
ethernet lmi interface configuration command	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.
any	Map all VLANs (untagged and VLANs 1 to 4094).
default	Map to the default service instance. You can use the default keyword only if you have already mapped the service instance to a VLAN or a group of VLANs.
untagged	Map only untagged VLANs.

Defaults

No E-LMI mapping parameters are defined.

Command Modes

Ethernet service configuration

Command History

Release	Modification
12.2(25)SEG	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).

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
service instance <i>id</i> ethernet	Defines an Ethernet service instance and enters Ethernet service configuration mode.
show ethernet service instance	Displays information about configured Ethernet service instances.

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	critical-event	Configure the switch to put an interface in error-disabled mode when an unspecified critical event has occurred.
	dying-gasp	Configure the switch to put an interface in error-disabled mode when an unrecoverable condition has occurred.
	link-fault	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(35)SE	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.
	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.
	The Catalyst 3750 Metro 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. It can respond to, but not generate, Dying Gasp PDUs based on loss of power.
	For complete command and configuration for the Ethernet OAM protocol, see the Cisco IOS feature module at this URL: http://www.cisco.com/en/US/products/ps6922/products_feature_guide09186a008067344c.html For documentation for the CFM and Ethernet OAM commands, see this URL: http://www.cisco.com/en/US/products/ps6922/products_command_reference_book09186a0080699104.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

Command	Description
show ethernet oam status [interface interface-id]	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

bundle	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.
all-to-one	(Optional) Configure the UNI to support bundling with a single EVC at the UNI and all CE VLANs mapped to that EVC.
multiplex	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(25)SEG	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
	show ethernet service interface	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(25)SEG	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
show ethernet service interface	Displays information about Ethernet service instances on an interface, including service type.

flowcontrol

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

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

flowcontrol receive {desired | off | on}


Note

The switch can only receive pause frames.

Syntax Description	receive	Sets whether the interface can receive flow-control packets from a remote device.
	desired	Allows an interface to operate with an attached device that is required to send flow-control packets or with an attached device that is not required to but can send flow-control packets.
	off	Turns off an attached device's ability to send flow-control packets to an interface.
	on	Allows 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
	12.1(14)AX	This command was introduced.

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

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

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

- **receive on** or **desired**: The port cannot send 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 2-5 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 2-5 *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-if)# flowcontrol receive off
```

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

Related Commands

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

interface port-channel

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

```
interface port-channel port-channel-number

no interface port-channel port-channel-number
```

Syntax Description	port-channel-number Port-channel number. The range is 1 to 12.

Defaults	No port-channel logical interfaces are defined.

Command Modes	Global configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines

For Layer 2 EtherChannels, you do not have to create a port-channel 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 when the channel group gets its first physical port. If you create the port-channel 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.
 - Do not configure a port that is an active member of an EtherChannel as an 802.1x port. If 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 guide for this release.

Examples

This example shows how to create port-channel 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
channel-group	Assigns an Ethernet port to an EtherChannel group.
show etherchannel	Displays EtherChannel information for a channel.
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 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.
<i>macro name</i>	Specify the name of a macro.

Defaults

This command has no default setting.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	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
- **port-channel** *port-channel-number* - *port-channel-number*, where *port-channel-number* is from 1 to 12

**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.

- **fastethernet** switch number (always 1)/module/{*first port*} - {*last port*}
- **gigabitethernet** switch number (always 1)/module/{*first port*} - {*last port*}

For physical interfaces:

- The switch number is always 1.
- The module number is 0 for 10/100 ports and standard SFP module slots and 1 for enhanced-services (ES) ports.
- The range is *type 1/module-number/number - number* (for example, **gigabitethernet 1/0/1 - 2**).

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

```
interface range gigabitethernet1/0/1 -2
```

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

```
interface range fastethernet1/0/3 , gigabitethernet1/0/1 - 2
interface range fastethernet1/0/3 -5, fastethernet1/0/7 -8
```

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 gigabitethernet1/0/1 - 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 gigabitethernet1/0/1 - 2
Switch(config)# interface range macro macro1
Switch(config-if-range)#
```

Related Commands

Command	Description
define interface-range	Creates an interface range macro.
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.

interface vlan

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

interface vlan *vlan-id*

no interface vlan *vlan-id*

Syntax Description

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

Defaults

The default VLAN interface is VLAN 1.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

You cannot delete the VLAN 1 interface.

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 ISL or 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.

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 a new SVI with 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
	show interfaces vlan <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.

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 ip access-list global configuration command.
in	Specify filtering on inbound packets.
out	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
12.1(14)AX	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.

You can use this command to apply an access list to a Layer 2 or Layer 3 interface. However, note these limitations for Layer 2 interfaces (port ACLs):

- You can only apply ACLs in the inbound direction; the **out** keyword is not supported for Layer 2 interfaces.
- You can only apply one IP ACL and one MAC ACL per interface.
- Layer 2 interfaces 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 takes precedence over a router ACL or 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 gigabitethernet1/0/1
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. For syntax information, select Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands .
	ip access-list	Configures a named ACL. For syntax information, select Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands .
	show access-lists	Displays ACLs configured on the switch.
	show ip access-lists	Displays IP ACLs configured on the switch. For syntax information, select Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands .
	show ip interface	Displays information about interface status and configuration. For syntax information, select Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands .

ip address

Use the **ip address** interface configuration command to set an IP address for the Layer 2 switch or 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**]

Syntax Description

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

Defaults

No IP address is defined.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)AX	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 determine 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 DHCP server and you remove the switch IP address by using the **no ip address** command, IP processing is disabled, and the BOOTP or 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 port on the Layer 3 switch:

```
Switch(config)# ip multicast-routing
Switch(config)# interface gigabitethernet1/0/1
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
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.

ip arp inspection filter vlan

Use the **ip arp inspection filter vlan** global configuration command on the switch stack or on a standalone switch 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**]

This command is available only if your switch is running the enhanced multilayer image (EMI).

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.
static	(Optional) Specify static 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(25)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
arp access-list	Defines an ARP ACL.
deny (ARP access-list configuration)	Denies an ARP packet based on matches against the DHCP bindings.
permit	Permits an ARP packet based on matches against the DHCP bindings.
show arp access-list	Displays detailed information about ARP access lists.
show ip arp inspection vlan <i>vlan-range</i>	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 on the switch stack or on a standalone switch 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

This command is available only if your switch is running the enhanced multilayer image (EMI).

Syntax Description

rate <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).
burst interval <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.
none	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(25)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.

The rate of incoming ARP packets on EtherChannel ports equals the sum of the incoming rate of ARP packets from all 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
show ip arp inspection interfaces	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 on the switch stack or on a standalone switch 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

entries <i>number</i>	Number of entries to be logged in the buffer. The range is 0 to 1024.
logs <i>number</i>	Number of entries needed in the specified interval to generate system messages.
interval <i>seconds</i>	For logs <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 interval <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(25)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 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
arp access-list	Defines an ARP access control list (ACL).
clear ip arp inspection log	Clears the dynamic ARP inspection log buffer.
ip arp inspection vlan logging	Controls the type of packets that are logged per VLAN.
show ip arp inspection log	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 on the switch stack or on a standalone switch 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

This command is available only if your switch is running the enhanced multilayer image (EMI).

Syntax Description

This command has no arguments or keywords.

Defaults

The interface is untrusted.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(25)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 gigabitethernet1/0/1
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
	ip arp inspection log-buffer	Configures the dynamic ARP inspection logging buffer.
	show ip arp inspection interfaces	Displays the trust state and the rate limit of ARP packets for the specified interface or all interfaces.
	show ip arp inspection log	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 on the switch stack or on a standalone switch 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

src-mac	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.
dst-mac	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.
ip	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 compared only in ARP responses.
allow-zeros	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(25)EY	This command was introduced.
12.2(37)SE	The allow-zero keyword was added.

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
show ip arp inspection vlan <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 on the switch stack or on a standalone switch 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*

This command is available only if your switch is running the enhanced multilayer image (EMI).

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(25)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, and 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
arp access-list	Defines an ARP access control list (ACL).
show ip arp inspection vlan <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 on the switch stack or on a standalone switch 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.
acl-match { matchlog none }	Specify that the logging of packets is based on access control list (ACL) matches. The keywords have these meanings: • matchlog—Log packets based on the logging configuration specified in the access control entry (ACE). If you specify the matchlog keyword in this command and the log keyword in the permit or deny Address Resolution Protocol (ARP) access-list configuration command, ARP packets permitted or denied by the ACL are logged. • none—Do not log packets that match ACLs.
dhcp-bindings { permit all none }	Specify the logging of packets is based on DHCP binding matches. The keywords have these meanings: • all—Log all packets that match DHCP bindings. • none—Do not log packets that match DHCP bindings. • permit—Log DHCP-binding permitted packets.
arp-probe	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(25)EY	This command was introduced.
12.2(37)SE	The arp-probe keyword was added.

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
arp access-list	Defines an ARP ACL.
clear ip arp inspection log	Clears the dynamic ARP inspection log buffer.
ip arp inspection log-buffer	Configures the dynamic ARP inspection logging buffer.
show ip arp inspection log	Displays the configuration and contents of the dynamic ARP inspection log buffer.
show ip arp inspection vlan <i>vlan-range</i>	Displays the configuration and the operating state of dynamic ARP inspection for the specified VLAN.

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(25)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
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	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.
vlan <i>vlan-id</i>	Specify a VLAN number. The range is from 1 to 4904.
<i>ip-address</i>	Specify an IP address.
interface <i>interface-id</i>	Specify an interface on which to add or delete a binding entry.
expiry <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(25)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 512 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
gigabitethernet1/0/1 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.

Related Commands	Command	Description
	ip dhcp snooping	Enables DHCP snooping on a VLAN.
	show ip dhcp snooping binding	Displays the dynamically configured bindings in the DHCP snooping binding database and the configuration information.
	show ip source binding	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 |
rcp://user@host/filename | tftp://host/filename} | timeout seconds | write-delay seconds}
```

```
no ip dhcp snooping database [timeout | write-delay]
```

Syntax Description		
flash://filename		Specify that the database agent or the binding file is in the flash memory.
ftp://user:password@host/filename		Specify that the database agent or the binding file is on an FTP server.
rcp://user@host/filename		Specify that the database agent or the binding file is on a Remote Control Protocol (RCP) server.
tftp://host/filename		Specify that the database agent or the binding file is on a TFTP server.
timeout seconds		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.
write-delay seconds		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(25)EY	This command was introduced.

Usage Guidelines

The DHCP snooping binding database can have up to 512 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 **ip dhcp snooping database flash:/filename** command to save the DHCP snooping binding database in the stack master NVRAM. The database is not saved in a stack member NVRAM.

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
```

This example shows how to store a binding file called file01.txt in the stack master NVRAM.

```
Switch(config)# ip dhcp snooping database flash:file01.txt
```

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

Related Commands

Command	Description
ip dhcp snooping	Enables DHCP snooping on a VLAN.
ip dhcp snooping binding	Configures the DHCP snooping binding database.
show ip dhcp snooping database	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(25)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.

Related Commands	Command	Description
	show ip dhcp snooping	Displays the DHCP snooping configuration.
	show ip dhcp snooping binding	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(25)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
```

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

Related Commands	Command	Description
	show ip dhcp snooping	Displays the DHCP snooping configuration.
	show ip dhcp snooping binding	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 on the switch 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

string <i>ASCII-string</i>	Specify a remote ID, using from 1 to 63 ASCII characters (no spaces).
hostname	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(25)SEE	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 will be 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
ip dhcp snooping vlan information option format-type circuit-id string	Configures the option-82 circuit-ID suboption.
show ip dhcp snooping	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

Syntax Description	<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

Command History	Release	Modification
	12.2(25)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.

Related Commands	Command	Description
	errdisable recovery	Configures the recover mechanism.
	show ip dhcp snooping	Displays the DHCP snooping configuration.
	show ip dhcp snooping binding	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(25)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: <pre>Switch(config-if)# ip dhcp snooping trust</pre> You can verify your settings by entering the show ip dhcp snooping privileged EXEC command.

Related Commands	Command	Description
	show ip dhcp snooping	Displays the DHCP snooping configuration.
	show ip dhcp snooping binding	Displays the DHCP snooping binding information.

ip dhcp snooping verify

Use the **ip dhcp snooping verify** 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(25)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
show ip dhcp snooping	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	vlan <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(25)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: <pre>Switch(config)# ip dhcp snooping vlan 10</pre> You can verify your settings by entering the show ip dhcp snooping privileged EXEC command.

Related Commands	Command	Description
	show ip dhcp snooping	Displays the DHCP snooping configuration.
	show ip dhcp snooping binding	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 on the switch 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 string** *ASCII-string*

no ip dhcp snooping vlan *vlan* **information option format-type circuit-id string**

Syntax Description	vlan <i>vlan</i>	Specify the VLAN ID. The range is 1 to 4094.
	string <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(25)SEE	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 circuit-ID suboption is the switch VLAN and port identifier, in the format **vlan-mod-port**. This command allows you to configure a string of ASCII characters to be the circuit ID.



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 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
```

You can verify your settings by entering the **show ip dhcp snooping** user EXEC command.

**Note**

The **show ip dhcp snooping** 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
ip dhcp snooping information option format remote-id	Configures the option-82 remote-ID suboption.
show ip dhcp snooping	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

Syntax Description	<i>profile number</i> The IGMP profile number to be applied. The range is 1 to 4294967295.

Defaults	No IGMP filters are applied.

Command Modes	Interface configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	You can apply IGMP filters only to Layer 2 physical interfaces; you cannot apply IGMP filters to routed ports, switch virtual interfaces (SVIs), or ports that belong to an EtherChannel group.
	An IGMP profile can be applied to one or more switch port interfaces, but one port can have only one profile applied to it.

Examples	This example shows how to apply IGMP profile 22 to a port.

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip igmp filter 22
```

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

Related Commands	Command	Description
	ip igmp profile	Configures the specified IGMP profile number.
	show ip dhcp snooping statistics	Displays the characteristics of the specified IGMP profile.
	show running-config interface interface-id	Displays the running configuration on the switch interface, including the IGMP profile (if any) that is applied to an interface. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands .

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.
action deny	When the maximum number of entries is in the IGMP snooping forwarding table, drop the next IGMP join report. This is the default action.
action replace	When the maximum number of entries is in the IGMP snooping forwarding table, replace the existing group with the new group for which the IGMP report was received.

Defaults

The default maximum number of groups is no limit.

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

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.
12.2(25)EY	The action , deny , and replace keywords were 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 gigabitethernet1/0/2
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 gigabitethernet2/0/1
Switch(config-if)# ip igmp max-groups action replace
```

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

Related Commands

Command	Description
show running-config interface <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 Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands .

ip igmp profile

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

```
ip igmp profile profile number
no ip igmp profile profile number
```

Syntax Description	profile number The IGMP profile number being configured. The range is 1 to 4294967295.				
Defaults	No IGMP profiles are defined. When configured, the default action for matching an IGMP profile is to deny matching addresses.				
Command Modes	Global configuration				
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.1(14)AX</td><td>This command was introduced.</td></tr></table>	Release	Modification	12.1(14)AX	This command was introduced.
Release	Modification				
12.1(14)AX	This command was introduced.				

Usage Guidelines

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

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

When entering a range, enter the low IP multicast address, a space, and the high IP multicast address. You can apply an IGMP profile to one or more Layer 2 interfaces, but each interface can have only one profile applied to it.

Examples

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

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

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

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

ip igmp snooping

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

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

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

Syntax Description

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

Defaults

IGMP snooping is globally enabled on the switch.
IGMP snooping is enabled on VLAN interfaces.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

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

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

Examples

This example shows how to globally enable IGMP snooping:

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

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

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

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

Related Commands

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

Command	Description
show ip igmp snooping mrouter	Displays the IGMP snooping router ports.
show ip igmp snooping querier	Displays the configuration and operation information for the IGMP querier configured on a switch.

ip igmp snooping querier

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

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

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

Syntax Description

vlan <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.
address <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.
max-response-time <i>response-time</i>	(Optional) Set the maximum time to wait for an IGMP querier report. The range is 1 to 25 seconds.
query-interval <i>interval-count</i>	(Optional) Set the interval between IGMP queriers. The range is 1 to 18000 seconds.
tcn query [count <i>count</i> interval <i>interval</i>]	(Optional) Set parameters related to Topology Change Notifications (TCNs). The keywords have these meanings: • count <i>count</i>—Set the number of TCN queries to be executed during the TCN interval time. The range is 1 to 10. • interval <i>interval</i>—Set the TCN query interval time. The range is 1 to 255.
timer expiry	(Optional) Set the length of time until the IGMP querier expires. The range is 60 to 300 seconds.
version <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(25)EY	This command was introduced.

Usage Guidelines

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

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

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

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

Examples

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

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

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

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

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

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

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

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

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

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

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

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

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

Related Commands

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

ip igmp snooping report-suppression

Use the **ip igmp snooping report-suppression** global configuration command to enable Internet Group Management Protocol (IGMP) report suppression. Use the **no** form of this command to disable IGMP report suppression and 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(25)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 mulitcast router query also includes requests for IGMPv3 reports, the switch forwards all IGMPv1, IGMPv2, and IGMPv3 reports for a group to the multicast devices.

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

Examples This example shows how to disable report suppression:

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

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

Related Commands

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

ip igmp snooping vlan immediate-leave

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

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

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

Syntax Description	<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
	12.1(14)AX	This command was introduced.

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

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

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

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

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

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

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

ip igmp snooping vlan mrouter

Use the **ip igmp snooping 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 {cgmp** | **pim-dvmrp**}}**

no ip igmp snooping vlan *vlan-id* mrouter {*interface interface-id* | learn {cgmp** | **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.
interface <i>interface-id</i>	Specify the next-hop interface to the multicast router. The keywords have these meanings: fastethernet <i>interface number</i>—a Fast Ethernet IEEE 802.3 interface. gigabitethernet <i>interface number</i>—a Gigabit Ethernet IEEE 802.3z interface. port-channel <i>interface number</i>—a channel interface. The range is 0 to 12.
learn {cgmp pim-dvmrp}	Specify the multicast router learning method. The keywords have these meanings: cgmp—Set the switch to learn multicast router ports by snooping on Cisco Group Management Protocol (CGMP) packets. pim-dvmrp—Set 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
12.1(14)AX	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 CGMP learn method is useful for reducing control traffic.

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 gigabitethernet1/0/2
```

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

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

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

Related Commands

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

ip igmp snooping vlan static

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

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

no ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id*

Syntax Description

<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.
interface <i>interface-id</i>	Specify the interface of the member port. The keywords have these meanings: • fastethernet <i>interface number</i>—a Fast Ethernet IEEE 802.3 interface. • gigabitethernet <i>interface number</i>—a Gigabit Ethernet IEEE 802.3z interface. • port-channel <i>interface number</i>—a channel interface. The range is 0 to 12.

Defaults

By default, there are no ports statically configured as members of a multicast group.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

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

The configuration is saved in NVRAM.

Examples

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

```
Switch(config)# ip igmp snooping vlan 1 static 0100.5e02.0203 interface
gigabitethernet1/0/1
Configuring port gigabitethernet1/0/1 on group 0100.5e02.0203
```

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

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

ip 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.
	vlan <i>vlan-id</i>	Specify a VLAN number. The range is from 1 to 4094.
	<i>ip-address</i>	Specify an IP address.
	interface <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(25)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
gigabitethernet1/0/1
```

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
gigabitethernet1/0/1
Switch(config)# ip source binding 0001.1357.0007 vlan 1 172.20.50.30 interface
gigabitethernet1/0/1
```

You can verify your settings by entering the **show ip source binding** privileged EXEC command.

Related Commands	Command	Description
	ip verify source	Enables IP source guard on an interface.
	show ip source binding	Displays the IP source bindings on the switch.
	show ip verify source	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. This command is available only when your switch is running the cryptographic (encrypted) software image. Use the **no** form of this command to return to the default setting.

ip ssh version [1 | 2]

no ip ssh version [1 | 2]

Syntax Description

1	(Optional) Configure the switch to run SSH Version 1 (SSHv1).
2	(Optional) Configure the switch to run SSH Version 2 (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(25)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
	show ip ssh	Displays if the SSH server is enabled and displays the version and configuration information for the SSH server. For syntax information, select Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Security Command Reference, Release 12.2 > Other Security Features > Secure Shell Commands .
	show ssh	Displays the status of the SSH server. For syntax information, select Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Security Command Reference, Release 12.2 > Other Security Features > Secure Shell Commands .

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(25)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
arp	Adds a permanent entry in the ARP table. For syntax information, see the Cisco IOS IP Addressing Services Command Reference, Release 12.4 > ARP Commands .
show arp	Displays the entries in the ARP table. For syntax information, see the Cisco IOS IP Addressing Services Command Reference, Release 12.4 > ARP Commands .

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(25)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
arp	Adds a permanent entry in the ARP table. For syntax information, see the Cisco IOS IP Addressing Services Command Reference, Release 12.4 > ARP Commands .
show arp	Displays the entries in the ARP table. For syntax information, see the Cisco IOS IP Addressing Services Command Reference, Release 12.4 > ARP Commands .

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 [port-security]

no ip verify source

Syntax Description	port-security (Optional) Enable IP source guard with IP and MAC address filtering. If you do not enter the port-security keyword, IP source guard with IP address filtering is enabled.	
Defaults	IP source guard is disabled.	
Command Modes	Interface configuration	
Command History	Release	Modification
	12.2(25)EY	This command was introduced.
Usage Guidelines	To enable IP source guard with source IP address filtering, use the ip verify source interface configuration command. To enable IP source guard with source IP and MAC address filtering, use the ip verify source port-security interface configuration command. 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: <pre>Switch(config-if)# ip verify source</pre> This example shows how to enable IP source guard with source IP and MAC address filtering: <pre>Switch(config-if)# ip verify source port-security</pre> You can verify your settings by entering the show ip source binding privileged EXEC command.	
Related Commands	Command	Description
	ip source binding	Configures static bindings on the switch.
	show ip verify source	Displays the IP source guard configuration on the switch or on a specific interface.

ip vrf (global configuration)

Use the **ip vrf** global configuration command to configure a virtual private network (VPN) routing/forwarding (VRF) routing table and to enter VRF configuration mode. Use the **no** form of this command to remove a VRF routing table and to return to global configuration mode.

ip vrf *vrf-name*

no ip vrf *vrf-name*



Note

The switch supports multiple VPN routing/forwarding instances in customer edge devices (multi-VRF CE).

Syntax Description

<i>vrf-name</i>	Name assigned to a VRF.

Defaults

No VRFs are defined.

No import or export lists are associated with a VRF.

No route maps are associated with a VRF.

Command Modes

Global configuration or router configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

Entering the **ip vrf** command enables the VRF configuration mode. These configuration commands are available:

- **default:** sets a command (description, export, import, maximum, route-target) to its default.
- **description:** describes the VRF (up to 80 characters).
- **exit:** exits VRF configuration mode and returns you to global configuration mode.
- **export map** *route-map*: sets a route map to be used as an export route map for the VRF.
- **import map** *route-map*: sets a route map to be used as an import route map for the VRF.
- **maximum routes** *limit* [*warn threshold* | **warn-only**]: limits the maximum number of routes in a VRF to prevent a provider edge (PE) router from importing too many routes. The range is from 1 to 4294967295; the threshold is a percentage of the limit, from 1 to 100.
- **no:** negates a command or sets its defaults.
- **rd:** specifies a Route Distinguisher (RD) as either ASN-relative, containing an autonomous system number and an arbitrary number, or IP-address-relative, containing an IP address and an arbitrary number.

- 16-bit AS number: your arbitrary 32-bit number (for example, 101:3)
- 32-bit IP address: your arbitrary 16-bit number (for example, 192.168.122.15:1.)
- **route-target {import | export | both} route-target-ext-community:** specifies target VPN extended communities. You can specify the target for export, import, or both.

To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

The switch supports a total of 26 VRFs and VPNs.

Use an import route map when an application requires finer control over the routes imported into a VRF than provided by the import and export extended communities configured for the importing and exporting VRF. The **import map** command associates a route map with the specified VRF. By using a route map, you can filter routes that are eligible for import into a VRF, based on the route target extended community attributes of the route. The route map might deny access to selected routes from a community that is on the import list.

If you set a maximum routes threshold, the switch rejects routes when the threshold limit is reached. If you enter **warn-only**, the switch issues a syslog error message when the maximum number of VRF routes exceeds the allowed limit, but still allows additional routes.

An RD creates routing and forwarding tables and specifies the default route distinguisher for a VPN. You must configure a route distinguisher for a VRF to be functional. The RD is added to the beginning of the customer's IPv4 prefixes to change them into globally unique VPN-IPv4 prefixes.

The route target specifies a target VPN extended community. Like a route-distinguisher, an extended community is composed of either an autonomous system number and an arbitrary number or an IP address and an arbitrary number.

The **ip vrf vrf-name** command creates a VRF routing table and a Cisco Express Forwarding (CEF) forwarding table, both named *vrf-name*. Associated with these tables is the default route distinguisher value *route-distinguisher*.

Examples

This example shows how to create the VRF named *vpn1*, enter VRF configuration mode, and import a route map to the VRF:

```
Switch(config)# ip vrf vpn1
Switch(config-vrf)# rd 100:2
Switch(config-vrf)# route-target both 100:2
Switch(config-vrf)# route-target import 100:1
```

Related Commands

Command	Description
ip vrf (interface configuration)	Associates a VRF routing table or a route map with an interface.
show ip route vrf	Displays the IP routing table associated with a VRF. For syntax information, select Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Switching Services Command Reference, Release 12.2 .
show ip vrf	Displays display the set of defined VRFs and associated interfaces. For syntax information, select Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Switching Services Command Reference, Release 12.2 .

ip vrf (interface configuration)

Use the **ip vrf** interface configuration command to associate a virtual private network (VPN) routing/forwarding (VRF) routing table or a route map with an interface. Use the **no** form of this command to disassociate the VRF routing table or route map.

ip vrf { **forwarding** *table-name* | **sitemap** *route-map-name* }

no ip vrf { **forwarding** *table-name* | **sitemap** *route-map-name* }



Note

The switch supports multiple VPN routing/forwarding instances in customer edge devices (multi-VRF CE).

Syntax Description

forwarding <i>table-name</i>	Specify a VRF forwarding table name for the interface.
sitemap <i>route-map-name</i>	Specify a VRF route map for routes received from this site.

Defaults

The default for an interface is the global routing table.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

Use the **ip vrf forwarding** command to associate an interface with a VRF. Executing this command on an interface removes the IP address. You should then reconfigure the IP address.

Examples

This example shows how to link the VRF named *vpn1* to a port:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip vrf forwarding vpn1
```

Related Commands

Command	Description
ip vrf (global configuration)	Configures a VRF routing table.
ip route vrf	Establishes static routes for a VRF. For syntax information, select Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Switching Services Command Reference, Release 12.2 .

Command	Description
show ip route vrf	Displays the IP routing table associated with a VRF. For syntax information, select Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Switching Services Command Reference, Release 12.2.
show ip vrf	Displays display the set of defined VRFs and associated interfaces. For syntax information, select Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Switching Services Command Reference, Release 12.2.

l2protocol-tunnel

Use the **l2protocol-tunnel** interface configuration command to enable tunneling of Layer 2 protocols on an access or 802.1Q tunnel port. You can enable tunneling for Cisco Discovery Protocol (CDP), 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. If no keyword is entered, tunneling is enabled for all three Layer 2 protocols. You can also enable point-to-point tunneling for Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), or UniDirectional Link Detection (UDLD) packets. Use the **no** form of this command to disable tunneling on the interface, to return to having no shutdown threshold, or to return to having no drop threshold.

l2protocol-tunnel [**cdp** | **stp** | **vtp**] [**point-to-point** [**pagp** | **lACP** | **udld**]] | [**shutdown-threshold** [**cdp** | **stp** | **vtp**] [**point-to-point** [**pagp** | **lACP** | **udld**]] *value*] | [**drop-threshold** [**cdp** | **stp** | **vtp**] [**point-to-point** [**pagp** | **lACP** | **udld**]] *value*]

no l2protocol-tunnel [**cdp** | **stp** | **vtp**] [**point-to-point** [**pagp** | **lACP** | **udld**]] | [**shutdown-threshold** [**cdp** | **stp** | **vtp**] [**point-to-point** [**pagp** | **lACP** | **udld**]] *value*] | [**drop-threshold** [**cdp** | **stp** | **vtp**] [**point-to-point** [**pagp** | **lACP** | **udld**]] *value*]

Syntax Description

cdp	(Optional) Enable tunneling of CDP, specify a shutdown threshold for CDP, or specify a drop threshold for CDP.
stp	(Optional) Enable tunneling of STP, specify a shutdown threshold for STP, or specify a drop threshold for STP.
vtp	(Optional) Enable tunneling of VTP, specify a shutdown threshold for VTP, or specify a drop threshold for VTP.
point-to-point	(Optional) Enable point-to-point tunneling of PAgP, LACP, and UDLD packets.
pagp	(Optional) Enable point-to-point tunneling of PAgP, specify a shutdown threshold for PAgP, or specify a drop threshold for PAgP.
lACP	(Optional) Enable point-to-point tunneling of LACP, specify a shutdown threshold for LACP, or specify a drop threshold for LACP.
udld	(Optional) Enable point-to-point tunneling of UDLD, specify a shutdown threshold for UDLD, or specify a drop threshold for UDLD.
shutdown-threshold	(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.
drop-threshold	(Optional) Set a drop threshold for the maximum rate of Layer 2 protocol packets per second to be received before an interface drops packets.
<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.



Note

Though visible in the command-line help strings, the **point-to-point** [**pagp** | **lACP** | **udld**] keywords are not supported.

Defaults

The default is that no Layer 2 protocol packets are tunneled.

If you enter the command with no keyword, the default is to tunnel CDP, 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 to have no shutdown threshold for the number of Layer 2 protocol packets.

The default is to have no drop threshold for the number of Layer 2 protocol packets.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.
12.1(14)AX1	Support was added for the point-to-point [pagp lACP udld] keywords.

Usage Guidelines

You must enter this command, with or without protocol types, to tunnel Layer 2 protocol packets.

Layer 2 protocol tunneling across a service-provider network ensures that Layer 2 protocol 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.

When Layer 2 protocol tunneling is enabled on ingress ports on a switch, egress trunk ports forward the tunneled packets with a special encapsulation. If you also enable Layer 2 protocol tunneling on the egress trunk port, this behavior is bypassed and the switch forwards control protocol data units (PDUs) without any processing or modification. The Layer 2 protocol-tunnel bypass feature can provide interoperability with third-party vendors. Bypass mode transparently forwards control PDUs to vendor switches that have different ways of controlling protocol tunneling.

You can enable Layer 2 protocol tunneling individually for CDP, STP, VTP, or for all three protocols.

You can enable Layer 2 protocol tunneling on ports that are configured as access ports, 802.1Q tunnel ports, or trunk ports. You cannot enable Layer 2 protocol tunneling on ports configured with switchport mode **dynamic auto** or **dynamic desirable**.

EtherChannel port groups are compatible with tunnel ports as long as the 802.1Q configuration is consistent within an EtherChannel port group.

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.

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.

Protocol tunneling is disabled by default but can be enabled for the individual protocols on 802.1Q tunnel ports, access ports, or trunk ports.

You can enable point-to-point protocol tunneling individually for PAgP, LACP, UDLD, or for all three protocols.

Loopback detection is not supported on Layer 2 protocol tunneling of PAgP, LACP, or UDLD packets.

**Caution**

PAgP, LACP, and UDLD protocol 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 serious network failure.

Dynamic Trunking Protocol (DTP) is not compatible with Layer 2 protocol tunneling because you must manually configure asymmetric links with tunnel ports and trunk ports.

Edge switches on the outbound side of the service-provider network restore the proper Layer 2 protocol and MAC address information and forward the packets to all tunnel, access, and Layer 2 protocol-enabled trunk ports in the same metro VLAN.

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 enabled 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 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
	l2protocol-tunnel cos	Configures a class of service (CoS) value for all tunneled Layer 2 protocol packets.
	show errdisable recovery	Displays errdisable recovery timer information.
	show l2protocol-tunnel	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 a class of service (CoS) value for all tunneled Layer 2 protocol packets. Use the **no** form of this command to return to the default value of 5.

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
12.1(14)AX	This command was introduced.

Usage Guidelines

When enabled, the tunneled Layer 2 protocol packets use the configured 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
show l2protocol-tunnel	Displays information about ports configured for Layer 2 protocol tunneling, including CoS.

lacp port-priority

Use the **lacp port-priority** interface configuration command to configure the port priority for the Link Aggregation Control Protocol (LACP). Use the **no** form of this command to return to the default setting.

lacp port-priority *priority*

no lacp port-priority

Syntax Description

priority Port priority for LACP. The range is 1 to 65535.

Defaults

The default is 32768.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The **lacp port-priority** interface configuration command determines which ports are bundled and which ports are put in hot-standby mode when there are more than eight ports in an LACP channel group.

An LACP channel group can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode.

In port-priority comparisons, a numerically *lower* value has a *higher* priority: When there are more than eight ports in an LACP channel-group, the eight ports with the numerically lowest values (highest priority values) for LACP port priority are bundled into the channel group, and the lower-priority ports are put in hot-standby mode. If two or more ports have the same LACP port priority (for example, they are configured with the default setting of 65535) an internal value for the port number determines the priority.



Note

The LACP port priorities are only effective if the ports are on the switch that controls the LACP link. See the **lacp system-priority** global configuration command for determining which switch controls the link.

Use the **show lacp internal** privileged EXEC command to display LACP port priorities and internal port number values.

For information about configuring LACP on physical ports, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

Examples

This example shows how to configure the LACP port priority on a port:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# lacp port-priority 1000
```

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

Related Commands

Command	Description
channel-group	Assigns an Ethernet port to an EtherChannel group.
lacp system-priority	Configures the LACP system priority.
show lacp <i>[channel-group-number]</i> internal	Displays internal information for all channel groups or for the specified channel group.

lACP system-priority

Use the **lACP system-priority** global configuration command to configure the system priority for the Link Aggregation Control Protocol (LACP). Use the **no** form of this command to return to the default setting.

lACP system-priority *priority*

no lACP system-priority

Syntax Description	priority	System priority for LACP. The range is 1 to 65535.
Defaults	The default is 32768.	
Command Modes	Global configuration	
Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines

The **lACP system-priority** command determines which switch in an LACP link controls port priorities. An LACP channel group can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode. When there are more than eight ports in an LACP channel-group, the switch on the controlling end of the link uses port priorities to determine which ports are bundled into the channel and which ports are put in hot-standby mode. Port priorities on the other switch (the noncontrolling end of the link) are ignored.

In priority comparisons, numerically lower values have higher priority. Therefore, the system with the numerically lower value (higher priority value) for LACP system priority becomes the controlling system. If both switches have the same LACP system priority (for example, they are both configured with the default setting of 32768), the LACP system ID (the switch MAC address) determines which switch is in control.

The **lACP system-priority** command applies to all LACP EtherChannels on the switch.

Use the **show etherchannel summary** privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag in the output display).

For more information about configuring LACP on physical ports, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

Examples This example shows how to set the LACP system priority:

```
Switch(config)# lACP system-priority 20000
```

You can verify your settings by entering the **show lACP sys-id** privileged EXEC command.

■ lacp system-priority

Related Commands	Command	Description
	channel-group	Assigns an Ethernet port to an EtherChannel group.
	lacp port-priority	Configures the LACP port priority.
	show lacp sys-id	Display 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 10. The default is 1.
	upstream	Configure a port as an upstream port for a specific link-state group.
	downstream	Configure a port as a downstream port for a specific link-state group.

Defaults The default group is group 1.

Command Modes Interface configuration

Command History	Release	Modification
	12.2(25)SEE	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 ten 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 fastethernet1/0/11 - 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
link state track	Enables a link-state group.
show link state group	Displays the link-state group information.
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 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*]

Syntax Description

<i>number</i>	(Optional) Specify the link-state group number. The group number can be 1 to 10. The default is 1.

Defaults

Link-state tracking is disabled for all groups.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)SEE	This command was introduced.

Usage Guidelines

Use the **link state track** global configuration command to enable a link-state group.

Examples

This example shows how enable link-state group 2:

```
Switch(config)# link state track 2
```

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

Related Commands

Command	Description
link state group	Configures an interface as a member of a link-state group.
show link state group	Displays the link-state group information.
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_comm_and_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 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

admin-tag	Configure administrative tag or site information.
civic-location	Configure civic location information.
elin-location	Configure emergency location information (ELIN).
identifier <i>id</i>	Specify the ID for the civic location or the elin location. The ID range is 1 to 4095.
<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(40)SE	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.

Use the **no lldp med-tlv-select location** information interface configuration command to disable the location TLV. The location TLV is enabled by default. For more information, see the “Configuring LLDP and LLDP-MED” chapter of the software configuration guide for this release.

Examples

This example shows how to configure civic location information on the switch:

```
Switch(config)# location civic-location identifier 1
Switch(config-civic)# number 3550
Switch(config-civic)# primary-road-name "Cisco Way"
Switch(config-civic)# city "San Jose"
Switch(config-civic)# state CA
Switch(config-civic)# building 19
Switch(config-civic)# room C6
Switch(config-civic)# county "Santa Clara"
Switch(config-civic)# country US
Switch(config-civic)# end
```

You can verify your settings by entering the **show location civic-location** privileged EXEC command.

This example shows how to configure the emergency location information location on the switch:

```
Switch (config)# location elin-location 14085553881 identifier 1
```

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

Related Commands

Command	Description
location (interface configuration)	Configures the location information for an interface.
show location	Displays the location information for an endpoint.

location (interface configuration)

Use the **location interface** command to enter location information for an interface. Use the **no** form of this command to remove the interface location information.

location { **additional-location-information** *word* | **civic-location-id** *id* | **elin-location-id** *id* }

no location { **additional-location-information** *word* | **civic-location-id** *id* | **elin-location-id** *id* }

Syntax Description

additional-location-information	Configure additional information for a location or place.
civic-location-id	Configure global civic location information for an interface.
elin-location-id	Configure emergency location information for an interface.
<i>id</i>	Specify the ID for the civic location or the elin location. The ID range is 1 to 4095.
<i>word</i>	Specify a word or phrase that provides additional location information.

Defaults

This command has no default setting.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(40)SE	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.

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
```

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
	location (global configuration)	Configures the location information for an endpoint.
	show location	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	bundle-status	Enable notification of BUNDLE and UNBUNDLE messages.
	link-status	Enable notification of interface data link status changes.
	spanning-tree	Enable notification of spanning-tree events.
	status	Enable notification of spanning-tree state change messages.
	trunk-status	Enable notification of trunk-status messages.

Defaults	Event logging is disabled.

Command Modes	Interface configuration

Command History	Release	Modification
	12.2(25)SEF	This command was introduced.

Examples	This example shows how to enable spanning-tree logging: <pre>Switch(config-if)# logging event spanning-tree</pre>

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: flash:
<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: • emergencies—System is unusable (severity 0). • alerts—Immediate action needed (severity 1). • critical—Critical conditions (severity 2). • errors—Error conditions (severity 3). • warnings—Warning conditions (severity 4). • notifications—Normal but significant messages (severity 5). • information—Information messages (severity 6). • debugging—Debugging messages (severity 7).

Defaults

The minimum file size is 2048 bytes; the maximum file size is 4096 bytes.

The default severity level is 7 (**debugging** messages and numerically lower levels).

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The log file is stored in ASCII text format in an internal buffer on the switch. You can access logged system messages by using the switch command-line interface (CLI) or by saving them to a properly configured syslog server. If the switch fails, the log is lost unless you had previously saved it to flash memory by using the **logging file flash:filename** global configuration command.

After saving the log to flash memory by using the **logging file flash:filename** global configuration command, you can use the **more flash:filename** privileged EXEC command to display its contents.

The command rejects the minimum file size if it is greater than the maximum file size minus 1024; the minimum file size then becomes the maximum file size minus 1024.

Specifying a *level* causes messages at that level and numerically lower levels to be displayed.

Examples

This example shows how to save informational log messages to a file in flash memory:

```
Switch(config)# logging file flash:logfile informational
```

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

Related Commands

Command	Description
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 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

Syntax Description

<i>name</i>	Specify a named MAC access list.
in	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
12.1(14)AX	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 a port:

```
Switch(config)# interface gigabitethernet1/0/1
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 view configured ACLs on the switch by entering the **show access-lists** privileged EXEC command.

Related Commands

Command	Description
show access-lists	Displays the ACLs configured on the switch.
show mac access-group	Displays the MAC ACLs configured on the switch.
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 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
12.1(14)AX	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 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](#) 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-mac1)#
```

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
deny	Configures the MAC ACL (in extended MAC-access list configuration mode).
permit	
show access-lists	Displays the access lists configured on the switch.
vlan access-map	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.
	<i>10-100000</i>	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
	12.1(14)AX	This command was introduced.

Usage Guidelines If hosts do not send continuously, increase the aging time to record the dynamic entries for a longer time. Increasing the time can reduce the possibility of flooding when the hosts send again.

If you do not specify a specific VLAN, this command sets the aging time for all VLANs.

Examples This example shows how to set the aging time to 200 seconds for all VLANs:

```
Switch(config)# mac address-table aging-time 200
```

You can verify your setting by entering the **show mac address-table aging-time** privileged EXEC command.

Related Commands	Command	Description
	show mac address-table aging-time	Displays the MAC address table aging time for all VLANs or the specified VLAN.

mac address-table learning

Use the **mac address-table learning** global configuration command to enable MAC address learning on a VLAN or on a Layer 3 port. Use the **no** form of this command to disable MAC address learning on a VLAN or Layer 3 interface to control which VLANs can learn MAC addresses.

```
mac address-table learning {vlan vlan-id | interface interface-id}

no mac address-table learning {vlan vlan-id | interface interface-id}
```

Syntax Description

vlan <i>vlan-id</i>	Specify a single VLAN ID or a range of VLAN IDs separated by a hyphen or command on which to apply the per-VLAN learning of all MAC addresses; valid values are from 1 to 4094. The VLAN cannot be an internal VLAN.
interface <i>interface-id</i>	Enter an interface for enabling per-interface based learning of all MAC addresses. The interface must be a Layer 3 interface used in port-based EoMPLS.

Defaults

By default, MAC address learning is enabled on all VLANs and disabled on interfaces.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)SEG	This command was introduced.
12.2(44)SE	The interface <i>interface-id</i> option was added.

Usage Guidelines

- Follow these guidelines for MAC address learning on VLANs:
- 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, **no 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 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 in 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 only 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 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.

Follow these guidelines for MAC address learning on Layer 3 ports:



Note

Do not use this command on interfaces other than Layer 3 interfaces used in port-based EoMPLS.

- MAC address learning is disabled by default on physical interfaces. You should enable it only on a Layer 3 interface in a port-based EoMPLS session.
- For port-based EoMPLS, the default disabled state does not allow bidirectional line-rate forwarding.
- Enabling MAC address learning on a Layer 3 EoMPLS port ensures that bidirectional traffic can occur at line rate. However, when MAC address learning is enabled, duplicate MAC addresses across VLANs are not supported. An example would be running HSRP groups across the port-based EoMPLS session.

Examples

This example shows how to disable MAC address learning on VLAN 2003:

```
Switch(config)# no mac address-table learning vlan 2003
```

This example shows how to enable MAC address learning on a Layer 3 interface to be used in port-based EoMPLS:

```
Switch(config)# mac address-table learning interface gigabitethernet1/1/1
```

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
show mac address-table learning	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	receive	Specify that the switch processes MAC address-table move update messages.
	transmit	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(25)SED	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:
	<pre>Switch# configure terminal Switch(conf)# mac address-table move update transmit Switch(conf)# end</pre>
	This example shows how to configure an uplink switch to get and process MAC address-table move update messages:
	<pre>Switch# configure terminal Switch(conf)# mac address-table move update receive Switch(conf)# end</pre> You can verify your settings by entering the show mac address-table move update privileged EXEC command.

Related Commands	Command	Description
	<code>clear mac address-table move update</code>	Clears the MAC address-table move update global counters.
	<code>show mac address-table move update</code>	Displays the MAC address-table move update information on the switch.
	<code>debug matm move update</code>	Debugs the MAC address-table move update message processing.

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 [**history-size** *value*] | [**interval** *value*]

no mac address-table notification [**history-size** | **interval**]

Syntax Description

history-size <i>value</i>	(Optional) Configure the maximum number of entries in the MAC notification history table. The range is 0 to 500 entries.
interval <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.

Defaults

By default, the MAC address notification feature is disabled.

The default trap interval value is 1 second.

The default number of entries in the history table is 1.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The MAC address notification 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 notifications are generated only for dynamic and secure MAC addresses. Events 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 feature by using the **mac address-table notification** command. You must also enable MAC address notification traps on an interface by using the **snmp trap mac-notification** interface configuration command and configure the switch to send MAC address traps to the NMS by using the **snmp-server enable traps mac-notification** global configuration command.

Examples

This example shows how to enable the **mac address-table notification** feature, set the interval time to 60 seconds, and set the history size to 100 entries:

```
Switch(config)# mac address-table notification
Switch(config)# mac address-table notification interval 60
Switch(config)# mac address-table notification history-size 100
```

You can verify your settings by entering the **show mac address-table notification** privileged EXEC command.

Related Commands	Command	Description
	clear mac address-table notification	Clears the MAC address notification global counters.
	show mac address-table notification	Displays the MAC address notification settings on all interfaces or on the specified interface.
	snmp-server enable traps	Sends the SNMP MAC notification traps when the mac-notification keyword is appended.
	snmp trap mac-notification	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 addresses from the table.

mac address-table static *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

no mac address-table static *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

Syntax Description	<i>mac-addr</i>	Destination MAC address (unicast or multicast) to add to the address table. Packets with this destination address received in the specified VLAN are forwarded to the specified interface.
	vlan <i>vlan-id</i>	Specify the VLAN in which the packet with the specified MAC address is received. The range is 1 to 4094.
	interface <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
	12.1(14)AX	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
gigabitethernet1/0/1
```

You can verify your setting by entering the **show mac address-table** privileged EXEC command.

Related Commands	Command	Description
	show mac address-table static	Displays static MAC address table entries only.

mac address-table static drop

Use the **mac address-table static drop** global configuration command to enable unicast MAC address filtering and to configure the switch to drop traffic with a specific source or destination MAC address. Use the **no** form of this command to return to the default setting.

mac address-table static *mac-addr* **vlan** *vlan-id* **drop**

no mac address-table static *mac-addr* **vlan** *vlan-id*

Syntax Description

<i>mac-addr</i>	Unicast source or destination MAC address. Packets with this MAC address are dropped.
vlan <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(25)EY	This command was introduced.

Usage Guidelines

Follow these guidelines when using this feature:

- Multicast MAC addresses, broadcast MAC addresses, and router MAC addresses are not supported. Packets that are forwarded to the CPU are also not supported.
- If you add a unicast MAC address as a static address and configure unicast MAC address filtering, the switch either adds the MAC address as a static address or drops packets with that MAC address, depending on which command was entered last. The second command that you entered overrides the first command.

For example, if you enter the **mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* global configuration command followed by the **mac address-table static** *mac-addr* **vlan** *vlan-id* **drop** command, the switch drops packets with the specified MAC address as a source or destination.

If you enter the **mac address-table static** *mac-addr* **vlan** *vlan-id* **drop** global configuration command followed by the **mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* command, the switch adds the MAC address as a static address.

Examples

This example shows how to enable unicast MAC address filtering and to configure the switch to drop packets that have a source or destination address of c2f3.220a.12f4. When a packet is received in VLAN 4 with this MAC address as its source or destination, the packet is dropped:

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop
```

This example shows how to disable unicast MAC address filtering:

```
Switch(config)# no mac address-table static c2f3.220a.12f4 vlan 4
```

You can verify your setting by entering the **show mac address-table static** privileged EXEC command.

Related Commands

Command	Description
show mac address-table static	Displays only static MAC address table entries.

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	apply	Apply a macro to the specified interface.
	trace	Use the trace keyword to apply a macro to an interface and to debug the macro.
	<i>macro-name</i>	Specify the name of the macro.
	parameter <i>value</i>	(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(25)EY	This command was introduced.

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.

There are Cisco-default Smartports macros embedded in the switch software. You can display these macros and the commands they contain by using the **show parser macro** user EXEC command.

Follow these guidelines when you apply a Cisco-default Smartports macro on an interface:

- Display all macros on the switch by using the **show parser macro** user EXEC command. Display the contents of a specific macro by using the **show parser macro name** *macro-name* user EXEC command.
- Keywords that begin with \$ mean that a unique parameter value is required. Append the Cisco-default macro with the required values by using the **parameter value** keywords.

The Cisco-default macros use the \$ character to help identify required keywords. There is no restriction on using the \$ character to define keywords when you create a macro.

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'
```

This example shows how to display the Cisco-default **cisco-desktop** macro and how to apply the macro and set the access VLAN ID to 25 on an interface:

```
Switch# show parser macro cisco-desktop
-----
Macro name : cisco-desktop
Macro type : default

# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access

# Enable port security limiting port to a single
# MAC address -- that of desktop
switchport port-security
switchport port-security maximum 1

# Ensure port-security age is greater than one minute
# and use inactivity timer
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
```

```
# Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable
-----
Switch#
Switch# configure terminal
Switch(config)# interface fastethernet1/0/4
Switch(config-if)# macro apply cisco-desktop $AVID 25
```

Related Commands

Command	Description
macro description	Adds a description about the macros that are applied to an interface.
macro global	Applies a macro on a switch or applies and traces a macro on a switch.
macro global description	Adds a description about the macros that are applied to the switch.
macro name	Creates a macro.
show parser macro	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*

Syntax Description

description *text* Enter a description about the macros that are applied to the specified interface.

Defaults

This command has no default setting.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(25)EY	This command was introduced.

Usage Guidelines

Use the **description** 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.

Related Commands

Command	Description
macro apply	Applies a macro on an interface or applies and traces a macro on an interface.
macro global	Applies a macro on a switch or applies and traces a macro on a switch
macro global description	Adds a description about the macros that are applied to the switch.
macro name	Creates a macro.
show parser macro	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	apply	Apply a macro to the switch.
	trace	Use the trace keyword to apply a macro to a switch and to debug the macro.
	<i>macro-name</i>	Specify the name of the macro.
	parameter value	(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(25)EY	This command was introduced.

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.

There are Cisco-default Smartports macros embedded in the switch software. You can display these macros and the commands they contain by using the **show parser macro** user EXEC command.

Follow these guidelines when you apply a Cisco-default Smartports macro on a switch:

- Display all macros on the switch by using the **show parser macro** user EXEC command. Display the contents of a specific macro by using the **show parser macro name** *macro-name* user EXEC command.
- Keywords that begin with \$ mean that a unique parameter value is required. Append the Cisco-default macro with the required values by using the **parameter** *value* keywords.

The Cisco-default macros use the \$ character to help identify required keywords. There is no restriction on using the \$ character to define keywords when you create a macro.

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 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
macro apply	Applies a macro on an interface or applies and traces a macro on an interface.
macro description	Adds a description about the macros that are applied to an interface.

Command	Description
macro global description	Adds a description about the macros that are applied to the switch.
macro name	Creates a macro.
show parser macro	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(25)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 udld aggressive mode enabled
```

You can verify your settings by entering the **show parser macro description** privileged EXEC command.

Related Commands

Command	Description
macro apply	Applies a macro on an interface or applies and traces a macro on an interface.
macro description	Adds a description about the macros that are applied to an interface.
macro global	Applies a macro on a switch or applies and traces a macro on a switch.
macro name	Creates a macro.
show parser macro	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(25)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 fa1/0/1
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
macro apply	Applies a macro on an interface or applies and traces a macro on an interface.
macro description	Adds a description about the macros that are applied to an interface.
macro global	Applies a macro on a switch or applies and traces a macro on a switch
macro global description	Adds a description about the macros that are applied to the switch.
show parser macro	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	ip address	Set the access map to match packets against an IP address access list.
	mac address	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
	12.1(14)AX	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 *al2*:

```
Switch(config)# vlan access-map vmap4
Switch(config-access-map)# match ip address al2
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# vlan filter vmap4 vlan-list 5-6
```

match (access-map configuration)

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

Related Commands	Command	Description
	access-list	Configures a standard numbered ACL. For syntax information, select Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands .
	action	Specifies the action to be taken if the packet matches an entry in an access control list (ACL).
	ip access list	Creates a named access list. For syntax information, select Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands .
	mac access-list extended	Creates a named MAC address access list.
	show vlan access-map	Displays the VLAN access maps created on the switch.
	vlan access-map	Creates a VLAN access map.

match (class-map configuration)

Use the **match** class-map configuration command to define the match criteria for a class map. Use the **no** form of this command to remove the match criteria.

```
match { access-group acl-index-or-name | cos [inner] cos-list | input-interface interface-id-list |  
         ip dscp dscp-list | ip precedence ip-precedence-list | mpls experimental exp-list | vlan [inner]  
         vlan-id }
```

```
no match { access-group acl-index-or-name | cos [inner] cos-list | input-interface interface-id-list  
           | ip dscp dsc-list | ip precedence ip-precedence-list | mpls experimental exp-list | vlan [inner]  
           vlan-id }
```

Syntax Description	
access-group <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.
cos [inner] <i>cos-list</i>	List of up to four Layer 2 class of service (CoS) values to match against a packet. Separate each value with a space. The range is 0 to 7. Use the inner keyword to match the inner CoS value in 802.1Q tunneling traffic (instead of matching the outer CoS value).
input-interface <i>interface-id-list</i>	Specify the physical ports to which the interface-level class map in a hierarchical dual-level policy map applies. This command can only be used in the child-level policy map and must be the only match condition in the child-level policy map. You can specify up to six entries in the list by specifying a port (counts as one entry), a list of ports separated by a space (each port counts as an entry), or a range of ports separated by a hyphen (counts as two entries).
ip dscp <i>dscp-list</i>	List of up to eight IP Differentiated Services Code Point (DSCP) values to match against a packet. Separate each value with a space. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value.
ip precedence <i>ip-precedence-list</i>	List of up to eight IP-precedence values to match against a packet. Separate each value with a space. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.
mpls experimental <i>exp-list</i>	List of up to eight multiprotocol label switching (MPLS) experimental values to match against a packet. Separate each value with a space. The range is 0 to 7.
vlan [inner] <i>vlan-id</i>	Match a packet based on the VLAN ID. The keywords have these meanings: vlan <i>vlan-id</i>—Match a packet based on the VLAN ID, or match a packet based on the outer VLAN ID if an 802.1Q tunnel is configured. You can specify a single VLAN identified by a VLAN number or a range of VLANs separated by a hyphen. The range is 1 to 4094. vlan inner <i>vlan-id</i>—Match a packet based on the inner VLAN ID of an 802.1Q tunnel. You can specify a single VLAN identified by a VLAN number or a range of VLANs separated by a hyphen. The range is 1 to 4094.

**Note**

Though visible in the command-line help strings, the **any**, **class-map**, **destination-address**, **not**, **protocol**, and **source-address** keywords are not supported.

Defaults

No match criteria are defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.
12.2(25)EY	The inner and the input-interface keywords were added.

Usage Guidelines

Before entering the **match** command, you must first enter the **class-map** global configuration command to specify the name of the class whose match criteria you want to establish. The **match** command is used to specify which fields in the packets are examined to classify the packets. If a packet matches the specified criteria, the packet is considered a member of the class and is forwarded according to the quality of service (QoS) specifications set in the traffic policy.

For the **match ip dscp dscp-list** or the **match ip precedence ip-precedence-list** command, you can enter a mnemonic name for a commonly used value. For example, you can enter the **match ip dscp af11** command, which is the same as entering the **match ip dscp 10** command. You can enter the **match ip precedence critical** command, which is the same as entering the **match ip precedence 5** command. For a list of supported mnemonics, enter the **match ip dscp ?** or the **match ip precedence ?** command to see the command-line help strings.

You can configure the **match cos [inner] cos-list**, **match ip dscp dscp-list**, **match ip precedence ip-precedence-list**, **match mpls experimental exp-list**, or the **match vlan** command in a class map within a policy map attached to an enhanced-services (ES) port. The **match access-group acl-index-or-name** command is not supported in an egress policy attached to an ES port or in a hierarchical ingress policy attached to an ES port. You can configure only the **match access-group acl-index-or-name** command and the **match input-interface interface-id-list** command in a single-level ingress policy map attached to a standard port or to an ES port.

The **match cos inner cos-list** command has no effect on non-802.1Q tunneling traffic.

If you want to match the CoS of traffic received on an ES port that is in 802.1Q tunneling mode, use the **match cos cos-list** command rather than the **match cos inner cos-list** command. The traffic is not tagged twice at the time that the match takes place.

You cannot mix VLAN-level and class-level matches within a class map.

To configure a class map that matches an 802.1Q tunneling pair (instead of matching a single VLAN), you must configure the **class-map** global configuration command with the **match-all** keyword. You must enter the **match vlan** command before the **match vlan inner** command.

If you enter the **match vlan** or the **match vlan inner** command, the **class-map match-any** command is not supported.

Use the **input-interface interface-id-list** keyword when you are configuring an interface-level class map in a hierarchical dual-level policy map. For the *interface-id-list*, you can specify up to six entries.

Packets that do not meet any of the matching criteria are classified as members of the default traffic class. You configure it by specifying **class-default** as the class name in the **class** policy-map configuration command. For more information, see the “[class](#)” section on page 2-35.

Examples

This example shows how to create a class map called *class2*, which matches all the inbound traffic with DSCP values of 10, 11, and 12:

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# exit
```

This example shows how to create a class map called *class3*, which matches all the inbound traffic with IP-precedence values of 5, 6, and 7:

```
Switch(config)# class-map class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# exit
```

This example shows how to create a class map called *dot1q*, which matches all outbound traffic with an outer VLAN ID of 5 and an inner VLAN ID of 3 to 8:

```
Switch(config)# class-map match-all dot1q
Switch(config-cmap)# match vlan 5
Switch(config-cmap)# match vlan inner 3 - 8
Switch(config-cmap)# exit
```

This example shows how to delete the IP-precedence match criteria and to classify traffic using *acl1*:

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# no match ip precedence
Switch(config-cmap)# match access-group acl1
Switch(config-cmap)# exit
```

This example shows how to specify a list of physical ports to which an interface-level class map in a hierarchical dual-level policy map applies:

```
Switch(config)# class-map match-all class4
Switch(config-cmap)# match input-interface gigabitethernet1/0/1 gigabitethernet1/0/2
Switch(config-cmap)# exit
```

This example shows how to specify a range of physical ports to which an interface-level class map in a dual-level policy map applies:

```
Switch(config)# class-map match-all class4
Switch(config-cmap)# match input-interface gigabitethernet1/0/1 - gigabitethernet1/0/2
Switch(config-cmap)# exit
```

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

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
show class-map	Displays 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

Syntax Description This command has no arguments or keywords.

Defaults The default is Auto-MDIX is enabled.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines When you enable Auto-MDIX on an interface, you must also set the interface speed and duplex to **auto**. 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 cable type (straight through or crossover) is incorrect. Auto-MDIX is supported on all 10/100 interfaces and on 10/100/1000BASE-T/TX small form-factor pluggable (SFP) module interfaces. It is not supported on 1000BASE-SX or -LX SFP module interfaces.



Caution

ES ports do not support 10 or 100 Mbps operation. If a 1000BASE-T SFP module is inserted in an ES module port, and you set the speed to **auto** to enable Auto-MDIX, be sure that the interface is connected to a Gigabit interface. Setting the speed to **auto** can result in severe data loss if the interface is connected to a 10/100 interface on another switch.

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

```
Switch# configure terminal
Switch(config)# interface fastethernet1/0/1
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.

mls qos

Use the **mls qos** global configuration command to enable quality of service (QoS) for the entire switch. When the **mls qos** command is entered, QoS is enabled with the default parameters on all ports in the system. Use the **no** form of this command to reset all the QoS-related statistics and to disable the QoS features for the entire switch.

mls qos

no mls qos

Syntax Description

This command has no arguments or keywords.

Defaults

QoS is disabled. There is no concept of trusted or untrusted ports because the packets are not modified (the CoS, DSCP, and IP precedence values in the packet are not changed). Traffic is switched in pass-through mode (packets are switched without any rewrites and classified as best effort without any policing).

When QoS is enabled with the **mls qos** global configuration command and all other QoS settings are set to their defaults, traffic is classified as best effort (the Differentiated Services Code Point [DSCP] and class of service [CoS] value is set to 0) without any policing. No policy maps are configured. The default port trust state on all ports is untrusted. The default ingress queue, egress queue-set, and hierarchical egress queue settings are in effect.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

QoS must be globally enabled to use QoS classification, policing, mark down or drop, queueing, and traffic shaping features. You can create a policy map and attach it to a port before entering the **mls qos** command. However, until you enter the **mls qos** command, QoS processing is disabled.

Policy maps and class maps used to configure QoS are not deleted from the configuration by the **no mls qos** command, but entries corresponding to policy maps are removed from the switch hardware to save system resources. To re-enable QoS with the previous configurations, use the **mls qos** command.

When QoS is disabled, ingress traffic is switched in pass-through mode, which means packets are switched without any rewrites and are classified to best effort without any policing.

Toggling the QoS status of the switch with this command modifies (reallocates) the sizes of the queues. During the queue size modification, the queue is temporarily shut down during the hardware reconfiguration, and the switch drops newly arrived packets for this queue.

Examples

This example shows how to enable QoS on the switch:

```
Switch(config)# mls qos
```

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

Related Commands

Command	Description
show mls qos	Displays QoS information.

mls qos aggregate-policer

Use the **mls qos aggregate-policer** global configuration command to define policer parameters, which can be shared by multiple classes within 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 delete an aggregate policer.

mls qos aggregate-policer *aggregate-policer-name* *rate-bps* *burst-byte* **exceed-action** {**drop** | **policed-dscp-transmit**}

no mls qos aggregate-policer *aggregate-policer-name*

Syntax Description

<i>aggregate-policer-name</i>	Name of the aggregate policer referenced by the police aggregate policy-map class configuration command.
<i>rate-bps</i>	Specify the average traffic rate in bps. The range is 8000 to 1000000000.
<i>burst-byte</i>	Specify the normal burst size in bytes. The range is 8000 to 1000000.
exceed-action drop	When the specified rate is exceeded, specify that the switch drop the packet.
exceed-action policed-dscp-transmit	When the specified rate is exceeded, specify that the switch change the Differentiated Services Code Point (DSCP) of the packet to that specified in the policed-DSCP map and then send the packet.

Defaults

No aggregate policers are defined.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The switch supports aggregate policers only in nonhierarchical single-level policy maps. Define an aggregate policer if the policer is shared with multiple classes.

Policers for a port cannot be shared with other policers for another port. Traffic from two different ports cannot be aggregated for policing purposes.

For standard port and enhanced-services (ES) ports, the port ASIC device that controls the ports supports 256 policers on the switch (255 user-configurable policers plus 1 policer reserved for system internal use). The maximum number of policers that can be configured per port is 63. Policers are allocated on demand by the software and are constrained by the hardware and ASIC boundaries. You cannot reserve policers per port (there is no guarantee that a port will be assigned to any policer).

You apply an aggregate policer to multiple classes in the same policy map. You cannot use an aggregate policer across different policy maps.

You cannot delete an aggregate policer if it is being used in a policy map. You must first use the **no police aggregate aggregate-policer-name** policy-map class configuration command to delete the aggregate policer from all policy maps before using the **no mls qos aggregate-policer aggregate-policer-name** command.

Ingress policing uses a token-bucket algorithm on a standard or an ES port. You configure the bucket depth (the maximum burst that is tolerated before the bucket overflows) by using the *burst-byte* option of the **police** policy-map class configuration command or the **mls qos aggregate-policer** global configuration command. You configure how fast (the average rate) the tokens are removed from the bucket by using the *rate-bps* option of the **police** policy-map class configuration command or the **mls qos aggregate-policer** global configuration command. For more information, see the software configuration guide for this release.

Examples

This example shows how to define the aggregate policer parameters and how to apply the policer to multiple classes in a policy map:

```
Switch(config)# mls qos aggregate-policer agg_policer1 10000 1000000 exceed-action drop
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# set ip dscp 10
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate agg_policer2
Switch(config-pmap-c)# exit
```

You can verify your settings by entering the **show mls qos aggregate-policer** privileged EXEC command.

Related Commands

Command	Description
police aggregate	Creates a policer that is shared by different classes.
show mls qos aggregate-policer	Displays the quality of service (QoS) aggregate policer configuration.

mls qos cos

Use the **mls qos cos** interface configuration command to define the default class of service (CoS) value of a port or to assign the default CoS to all inbound packets on the port. Use the **no** form of this command to return to the default setting.

```
mls qos cos {default-cos | override}

no mls qos cos {default-cos | override}
```

Syntax Description

<i>default-cos</i>	Assign a default CoS value to a port. If packets are untagged, the default CoS value becomes the packet CoS value. The CoS range is 0 to 7.
override	Override the CoS of the inbound packets, and apply the default CoS value on the port to all inbound packets.

Defaults

The default CoS value for a port is 0.
CoS override is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

You can use the default value to assign a CoS and Differentiated Services Code Point (DSCP) value to all inbound packets that are untagged (if the inbound packet does not have a CoS value). You also can assign a default CoS and DSCP value to all inbound packets by using the **override** keyword.

Use the **override** keyword when all inbound packets on certain ports deserve higher or lower priority than packets entering from other ports. Even if a port is previously set to trust DSCP, CoS, or IP precedence, this command overrides the previously configured trust state, and all the inbound CoS values are assigned the default CoS value configured with the **mls qos cos** command. If an inbound packet is tagged, the CoS value of the packet is modified with the default CoS of the port at the ingress port.

Examples

This example shows how to configure the default port CoS to 4 on a port:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# mls qos cos 4
```

This example shows how to assign all the packets entering a port to the default port CoS value of 4 on a port:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mls qos cos 4
Switch(config-if)# mls qos cos override
```

You can verify your settings by entering the **show mls qos interface** privileged EXEC command.

Related Commands

Command	Description
show mls qos interface	Displays quality of service (QoS) information at the port level.

mls qos dscp-mutation

Use the **mls qos dscp-mutation** interface configuration command to apply a Differentiated Services Code Point (DSCP)-to-DSCP-mutation map to a DSCP-trusted port. Use the **no** form of this command to return the map to the default settings (no DSCP mutation).

```
mls qos dscp-mutation dscp-mutation-name

no mls qos dscp-mutation dscp-mutation-name
```

Syntax Description	dscp-mutation-name	Name of the DSCP-to-DSCP-mutation map. This map was previously defined with the mls qos map dscp-mutation global configuration command.

Defaults	The default DSCP-to-DSCP-mutation map is a null map, which maps inbound DSCP values to the same DSCP values.	

Command Modes	Interface configuration	

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines

If two quality of service (QoS) domains have different DSCP definitions, use the DSCP-to-DSCP-mutation map to translate one set of DSCP values to match the definition of another domain. You apply the DSCP-to-DSCP-mutation map to the receiving port (ingress mutation) at the boundary of a QoS administrative domain.

With ingress mutation, the new DSCP value overwrites the one in the packet, and QoS handles the packet with this new value. The switch sends the packet out the port with the new DSCP value.

You can configure multiple DSCP-to-DSCP-mutation maps on ingress ports.

You apply the map only to DSCP-trusted ports. If you apply the DSCP mutation map to an untrusted port, to a class of service (CoS) or an IP-precedence trusted port, the command has no immediate effect until the port becomes DSCP-trusted.

When port trust policies are used with 802.1Q tunneling, all ports sharing the same tunnel VLAN must be configured with the same trust policy, and the ports involved must use the same DSCP-to-DSCP mutation map. For more information, see the [“mls qos map” section on page 2-252](#) and the [“mls qos trust” section on page 2-279](#).

Examples

This example shows how to define the DSCP-to-DSCP-mutation map named *dscpmutation1* and to apply the map to a port:

```
Switch(config)# mls qos map dscp-mutation dscpmutation1 10 11 12 13 to 30
Switch(config)# interface gigabitethernet1/0/1
```



```
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation dscpmutation1
```

This example show how to remove the DSCP-to-DSCP-mutation map name *dscpmutation1* from the port and to reset the map to the default:

```
Switch(config-if)# no mls qos dscp-mutation dscpmutation1
```

You can verify your settings by entering the **show mls qos maps** privileged EXEC command.

Related Commands	Command	Description
	mls qos map dscp-mutation	Defines the DSCP-to-DSCP-mutation map.
	mls qos trust	Configures the port trust state.
	show mls qos maps	Displays QoS mapping information.

mls qos enhanced

Use the **mls qos enhanced** interface configuration command to take the internal bandwidth from one enhanced-services (ES) port and apply it to the other ES port. Use the **no** form of this command to return to the default setting.

mls qos enhanced

no mls qos enhanced

Syntax Description This command has no arguments or keywords

Defaults The internal bandwidth is shared between the ES ports.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines

You can apply this command to only one ES port at a time. Applying the bandwidth to only a single ES port enables the existing quality of service (QoS) features to function more effectively.

Before applying this command to an ES port, disable the other ES port by using the **shutdown** interface configuration command. As long as the enhanced QoS functionality is applied to one ES port, the other ES port cannot be brought back up.

When you configure an ES port with the **mls qos enhanced** command, the port goes down and comes back up.

Examples

This example shows how to apply the internal bandwidth to one ES port:

```
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# shutdown
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/1/2
Switch(config-if)# mls qos enhanced
```

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

Related Commands	Command	Description
	show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.

mls qos map

Use the **mls qos map** global configuration command to define the class of service (CoS)-to-Differentiated Services Code Point (DSCP) map, the DSCP-to-CoS map, the DSCP-to-DSCP-mutation map, the IP-precedence-to-DSCP map, and the policed-DSCP map. Use the **no** form of this command to return to the default map.

```
mls qos map {cos-dscp dscp1...dscp8 | dscp-cos dscp-list to cos | dscp-mutation
dscp-mutation-name in-dscp to out-dscp | ip-prec-dscp dscp1...dscp8 | policed-dscp dscp-list
to mark-down-dscp}
```

```
no mls qos map {cos-dscp | dscp-cos | dscp-mutation dscp-mutation-name | ip-prec-dscp |
policed-dscp}
```

Syntax Description

cos-dscp <i>dscp1...dscp8</i>	Define the CoS-to-DSCP map. For <i>dscp1...dscp8</i>, enter eight DSCP values that correspond to CoS values 0 to 7. Separate each DSCP value with a space. The range is 0 to 63.
dscp-cos <i>dscp-list</i> to <i>cos</i>	Define the DSCP-to-CoS map. For <i>dscp-list</i>, enter up to eight DSCP values, with each value separated by a space. The range is 0 to 63. Then enter the to keyword. For <i>cos</i>, enter a single CoS value to which the DSCP values correspond. The range is 0 to 7.
dscp-mutation <i>dscp-mutation-name in-dscp</i> to <i>out-dscp</i>	Define the DSCP-to-DSCP-mutation map. For <i>dscp-mutation-name</i>, enter the mutation map name. For <i>in-dscp</i>, enter up to eight DSCP values, with each value separated by a space. Then enter the to keyword. For <i>out-dscp</i>, enter a single DSCP value. The range is 0 to 63.
ip-prec-dscp <i>dscp1...dscp8</i>	Define the IP-precedence-to-DSCP map. For <i>dscp1...dscp8</i>, enter eight DSCP values that correspond to the IP precedence values 0 to 7. Separate each DSCP value with a space. The range is 0 to 63.
policed-dscp <i>dscp-list</i> to <i>mark-down-dscp</i>	Define the policed-DSCP map. For <i>dscp-list</i>, enter up to eight DSCP values, with each value separated by a space. Then enter the to keyword. For <i>mark-down-dscp</i>, enter the corresponding policed (marked down) DSCP value. The range is 0 to 63.

Defaults

Table 2-6 shows the default CoS-to-DSCP map:

Table 2-6 *Default CoS-to-DSCP Map*

CoS Value	DSCP Value
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

Table 2-7 shows the default DSCP-to-CoS map:

Table 2-7 *Default DSCP-to-CoS Map*

DSCP Value	CoS Value
0–7	0
8–15	1
16–23	2
24–31	3
32–39	4
40–47	5
48–55	6
56–63	7

Table 2-8 shows the default IP-precedence-to-DSCP map:

Table 2-8 *Default IP-Precedence-to-DSCP Map*

IP Precedence Value	DSCP Value
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

The default DSCP-to-DSCP-mutation map is a null map, which maps an inbound DSCP value to the same DSCP value.

The default policed-DSCP map is a null map, which maps an inbound DSCP value to the same DSCP value.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

All the maps are globally defined. All the maps, except the DSCP-to-DSCP-mutation map, are applied to all ports. The DSCP-to-DSCP-mutation map is applied to a specific port.

Examples

This example shows how to define the IP-precedence-to-DSCP map and to map IP-precedence values 0 to 7 to DSCP values of 0, 10, 20, 30, 40, 50, 55, and 60:

```
Switch(config)# mls qos map ip-prec-dscp 0 10 20 30 40 50 55 60
```

This example shows how to define the policed-DSCP map. DSCP values 1, 2, 3, 4, 5, and 6 are marked down to DSCP value 0. Marked DSCP values that not explicitly configured are not modified.

```
Switch(config)# mls qos map policed-dscp 1 2 3 4 5 6 to 0
```

This example shows how to define the DSCP-to-CoS map. DSCP values 20, 21, 22, 23, and 24 are mapped to CoS 1. DSCP values 10, 11, 12, 13, 14, 15, 16, and 17 are mapped to CoS 0.

```
Switch(config)# mls qos map dscp-cos 20 21 22 23 24 to 1
Switch(config)# mls qos map dscp-cos 10 11 12 13 14 15 16 17 to 0
```

This example shows how to define the CoS-to-DSCP map. CoS values 0 to 7 are mapped to DSCP values 0, 5, 10, 15, 20, 25, 30, and 35.

```
Switch(config)# mls qos map cos-dscp 0 5 10 15 20 25 30 35
```

This example shows how to define the DSCP-to-DSCP-mutation map. All the entries that are not explicitly configured are not modified (remain as specified in the null map).

```
Switch(config)# mls qos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 10
Switch(config)# mls qos map dscp-mutation mutation1 8 9 10 11 12 13 to 10
Switch(config)# mls qos map dscp-mutation mutation1 20 21 22 to 20
Switch(config)# mls qos map dscp-mutation mutation1 0 31 32 33 34 to 30
```

You can verify your settings by entering the **show mls qos maps** privileged EXEC command.

Related Commands

Command	Description
mls qos dscp-mutation	Applies a DSCP-to-DSCP-mutation map to a DSCP-trusted port.
show mls qos maps	Displays quality of service (QoS) mapping information.

mls qos queue-set output buffers

Use the **mls qos queue-set output buffers** global configuration command to allocate buffers to a queue-set (four egress queues per port). Use the **no** form of this command to return to the default setting.

mls qos queue-set output *qset-id* buffers *allocation1* ... *allocation4*

no mls qos queue-set output *qset-id* buffers

Syntax Description	<i>qset-id</i>	ID of the queue-set. Each port belongs to a queue-set, which defines all the characteristics of the four egress queues per port. The range is 1 to 2.
	<i>allocation1</i> ... <i>allocation4</i>	Buffer space allocation (percentage) for each queue (four values for queues 1 to 4). For <i>allocation1</i> , <i>allocation3</i> , and <i>allocation4</i> , the range is 0 to 99. For <i>allocation2</i> , the range is 1 to 100 (including the CPU buffer). Separate each value with a space.

Defaults All allocation values are equally mapped among the four queues (25, 25, 25, 25). Each queue has 1/4 of the buffer space.

Command Modes Global configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.
	12.2(25)EY	The range for <i>allocation1</i> , <i>allocation3</i> , and <i>allocation4</i> changed from 0 to 100 to 0 to 99. The range for <i>allocation2</i> changed from 20 to 100 to 1 to 100.

Usage Guidelines Specify four allocation values, and separate each with a space.

Allocate buffers according to the importance of the traffic. For example, give a larger percentage of the buffer to the queue with the highest-priority traffic.

To configure different classes of traffic with different characteristics, use this command with the **mls qos queue-set output *qset-id* threshold** global configuration command.



Note

The egress queue-set default settings are suitable for most situations. You should change them only when you have a thorough understanding of the queues and if these settings do not meet your quality of service (QoS) solution.

Examples This example shows how to map a port to queue-set 2. It allocates 40 percent of the buffer space to egress queue 1 and 20 percent each to egress queues 2, 3, and 4.

```
Switch(config)# mls qos queue-set output 2 buffers 40 20 20 20
Switch(config)# interface fastethernet1/0/1
Switch(config-if)# queue-set 2
```

You can verify your settings by entering the **show mls qos interface** *[interface-id]* **buffers** or the **show mls qos queue-set** privileged EXEC command.

Related Commands	Command	Description
	mls qos queue-set output threshold	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
	queue-set	Maps a port to a queue-set.
	show mls qos interface buffers	Displays buffer allocation information.
	show mls qos queue-set	Displays settings for the queue-set.

mls qos queue-set output threshold

Use the **mls qos queue-set output threshold** global configuration command to configure the weighted tail-drop (WTD) thresholds, to guarantee the availability of buffers, and to configure the maximum memory allocation to a queue-set (four egress queues per port). Use the **no** form of this command to return to the default setting.

mls qos queue-set output *qset-id* **threshold** *queue-id* *drop-threshold1* *drop-threshold2*
reserved-threshold *maximum-threshold*

no mls qos queue-set output *qset-id* **threshold** [*queue-id*]

Syntax Description

<i>qset-id</i>	ID of the queue-set. Each port belongs to a queue-set, which defines all the characteristics of the four egress queues per port. The range is 1 to 2.
<i>queue-id</i>	Specific queue in the queue-set on which the command is performed. The range is 1 to 4.
<i>drop-threshold1</i> <i>drop-threshold2</i>	Two WTD thresholds expressed as a percentage of the allocated queue memory. The range is 1 to 400 percent.
<i>reserved-threshold</i>	Amount of memory to be guaranteed (reserved) for the queue and expressed as a percentage of the allocated memory. The range is 1 to 100 percent.
<i>maximum-threshold</i>	Enable a full queue to obtain more buffers than are reserved for it. This is the maximum memory that the queue can have before the packets are dropped. The range is 1 to 400 percent.

Defaults

When quality of service (QoS) is enabled, WTD is enabled.

[Table 2-9](#) shows the default WTD threshold settings.

Table 2-9 Default Egress Queue-Set WTD Threshold Settings

Feature	Queue 1	Queue 2	Queue 3	Queue 4
WTD drop threshold 1	100 percent	50 percent	100 percent	100 percent
WTD drop threshold 2	100 percent	50 percent	100 percent	100 percent
Reserved threshold	50 percent	100 percent	50 percent	50 percent
Maximum threshold	400 percent	400 percent	400 percent	400 percent

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

Use the **mls qos queue-set output *qset-id* buffers** global configuration command to allocate a fixed number of buffers to the four queues in a queue-set.

The drop-threshold percentages can exceed 100 percent and can be up to the maximum (if the maximum threshold exceeds 100 percent).

**Note**

The egress queue-set default settings are suitable for most situations. You should change them only when you have a thorough understanding of the queues and if these settings do not meet your QoS solution.

The switch uses a buffer allocation scheme to reserve a minimum amount of buffers for each egress queue-set, to prevent any queue or port from consuming all the buffers and depriving other queues, and to control whether to grant buffer space to a requesting queue. The switch detects whether or not the target queue has consumed more buffers than its reserved amount (under-limit), whether it has consumed all of its maximum buffers (over-limit), and whether the common pool is empty (no free buffers) or not empty (free buffers). If the queue is not over-limit, the switch can allocate buffer space from the reserved pool or from the common pool (if it is not empty). If there are no free buffers in the common pool or if the queue is over-limit, the switch drops the frame.

Examples

This example shows how to map a port to queue-set 2. It configures the drop thresholds for queue 2 to 40 and 60 percent of the allocated memory, guarantees (reserves) 100 percent of the allocated memory, and configures 200 percent as the maximum memory that this queue can have before packets are dropped.

```
Switch(config)# mls qos queue-set output 2 threshold 2 40 60 100 200
Switch(config)# interface fastethernet1/0/1
Switch(config-if)# queue-set 2
```

You can verify your settings by entering the **show mls qos interface *[interface-id]* buffers** or the **show mls qos queue-set** privileged EXEC command.

Related Commands

Command	Description
mls qos queue-set output buffers	Allocates buffers to a queue-set.
queue-set	Maps a port to a queue-set.
show mls qos interface buffers	Displays buffer allocation information.
show mls qos queue-set	Displays settings for the queue-set.

mls qos rewrite ip dscp

Use the **mls qos rewrite ip dscp** global configuration command to configure the switch to change (rewrite) the Differentiated Services Code Point (DSCP) field of an incoming IP packet. Use the **no** form of this command to configure the switch to not modify (rewrite) the DSCP field of the packet and to enable DSCP transparency.

mls qos rewrite ip dscp

no mls qos rewrite ip dscp

Syntax Description

This command has no arguments or keywords.

Defaults

DSCP transparency is disabled. The switch changes the DSCP field of the incoming IP packet.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX2	This command was introduced.

Usage Guidelines

DSCP transparency affects only the DSCP field of a packet at the egress. If DSCP transparency is enabled by using the **no mls qos rewrite ip dscp** command, the switch does not modify the DSCP field in the incoming packet, and the DSCP field in the outgoing packet is the same as that in the incoming packet.



Note

If a hierarchical service policy is applied to an enhanced-services (ES) port and includes a policy map to modify the DSCP value of the packet, the switch modifies the DSCP value regardless of the DSCP transparency configuration.

By default, DSCP transparency is disabled. The switch modifies the DSCP field in an incoming packet, and the DSCP field in the outgoing packet is based on the quality of service (QoS) configuration, including the port trust setting, policing and marking, and the DSCP-to-DSCP mutation map.

Regardless of the DSCP transparency configuration, the switch modifies the internal DSCP value of the packet that the switch uses to generate a class of service (CoS) value representing the priority of the traffic. The switch also uses the internal DSCP value to select an egress queue and threshold.

For example, if QoS is enabled and an incoming packet has a DSCP value of 32, the switch might modify the internal DSCP value based on the policy-map configuration and change the internal DSCP value to 16. If DSCP transparency is enabled, the outgoing DSCP value is 32 (same as the incoming value). If DSCP transparency is disabled, the outgoing DSCP value is 16 because it is based on the internal DSCP value.

Examples

This example shows how to enable DSCP transparency and configure the switch to not change the DSCP value of the incoming IP packet:

```
Switch(config)# mls qos
Switch(config)# no mls qos rewrite ip dscp
Switch(config-if)# end
```

This example shows how to disable DSCP transparency and configure the switch to change the DSCP value of the incoming IP packet:

```
Switch(config)# mls qos
Switch(config)# mls qos rewrite ip dscp
Switch(config-if)# end
```

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

Related Commands

Command	Description
mls qos	Enables QoS globally.
show mls qos interface	Displays QoS information at an interface level.

mls qos srr-queue input bandwidth

Use the **mls qos srr-queue input bandwidth** global configuration command to assign shaped round robin (SRR) weights to an ingress queue. The ratio of the weights is the ratio of the frequency in which the SRR scheduler sends packets from each queue. Use the **no** form of this command to return to the default setting.

mls qos srr-queue input bandwidth *weight1 weight2*

no mls qos srr-queue input bandwidth

Syntax Description	<i>weight1 weight2</i>	Ratio of <i>weight1</i> and <i>weight2</i> controls the ratio of the frequency in which the SRR scheduler sends packets from ingress queues 1 and 2. The range is 1 to 100. Separate each value with a space.

Defaults	Weight1 and weight2 are 4 (1/2 of the bandwidth is equally shared between the two queues).

Command Modes	Global configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	SRR services the priority queue for its configured weight as specified by the bandwidth keyword in the mls qos srr-queue input priority-queue <i>queue-id</i> bandwidth <i>weight</i> global configuration command. Then SRR shares the remaining bandwidth with both ingress queues and services them as specified by the weights configured with the mls qos srr-queue input bandwidth <i>weight1 weight2</i> global configuration command.

You specify which ingress queue is the priority queue by using the **mls qos srr-queue input priority-queue** global configuration command.

Examples	This example shows how to assign the ingress bandwidth for the queues. Priority queueing is disabled, and the shared bandwidth ratio allocated to queue 1 is 25/(25+75) and to queue 2 is 75/(25+75).

```
Switch(config)# mls qos srr-queue input priority-queue 2 bandwidth 0
Switch(config)# mls qos srr-queue input bandwidth 25 75
```

In this example, queue 2 has three times the bandwidth of queue 1; queue 2 is serviced three times as often as queue 1.

This example shows how to assign the ingress bandwidths for the queues. Queue 1 is the priority queue with 10 percent of the bandwidth allocated to it. The bandwidth ratio allocated to queues 1 and 2 is 4/(4+4). SRR services queue 1 (the priority queue) first for its configured 10 percent bandwidth. Then SRR equally shares the remaining 90 percent of the bandwidth between queues 1 and 2 by allocating 45 percent to each queue.

```
Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config)# mls qos srr-queue input bandwidth 4 4
```

You can verify your settings by entering the **show mls qos interface** *[interface-id]* **queueing** or the **show mls qos input-queue** privileged EXEC command.

Related Commands

Command	Description
mls qos srr-queue input buffers	Allocates the buffers between the ingress queues.
mls qos srr-queue input cos-map	Maps class of service (CoS) values to an ingress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue input dscp-map	Maps Differentiated Services Code Point (DSCP) values to an ingress queue or maps DSCP values to a queue and to a threshold ID.
mls qos srr-queue input priority-queue	Configures the ingress priority queue and guarantees bandwidth.
mls qos srr-queue input threshold	Assigns weighted tail-drop (WTD) threshold percentages to an ingress queue.
show mls qos input-queue	Displays ingress queue settings.
show mls qos interface queueing	Displays queueing strategy information.

mls qos srr-queue input buffers

Use the **mls qos srr-queue input buffers** global configuration command to allocate the buffers between the ingress queues. Use the **no** form of this command to return to the default setting.

mls qos srr-queue input buffers *percentage1 percentage2*

no mls qos srr-queue input buffers

Syntax Description	<i>percentage1</i> <i>percentage2</i>	Percentage of buffers allocated to ingress queues 1 and 2. The range is 0 to 100. Separate each value with a space.

Defaults	Ninety percent of the buffers is allocated to queue 1, and 10 percent of the buffers is allocated to queue 2.

Command Modes	Global configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	You should allocate the buffers so that the queues can handle any inbound bursty traffic.

Examples	This example shows how to allocate 60 percent of the buffer space to ingress queue 1 and 40 percent of the buffer space to ingress queue 2:

```
Switch(config)# mls qos srr-queue input buffers 60 40
```

You can verify your settings by entering the **show mls qos interface** *[interface-id]* **buffers** or the **show mls qos input-queue** privileged EXEC command.

Related Commands	Command	Description
	mls qos srr-queue input bandwidth	Assigns shaped round robin (SRR) weights to an ingress queue.
	mls qos srr-queue input cos-map	Maps class of service (CoS) values to an ingress queue or maps CoS values to a queue and to a threshold ID.
	mls qos srr-queue input dscp-map	Maps Differentiated Services Code Point (DSCP) values to an ingress queue or maps DSCP values to a queue and to a threshold ID.
	mls qos srr-queue input priority-queue	Configures the ingress priority queue and guarantees bandwidth.
	mls qos srr-queue input threshold	Assigns weighted tail-drop (WTD) threshold percentages to an ingress queue.

Command	Description
show mls qos input-queue	Displays ingress queue settings.
show mls qos interface buffers	Displays buffer allocation information.

mls qos srr-queue input cos-map

Use the **mls qos srr-queue input cos-map** global configuration command to map class of service (CoS) values to an ingress queue or to map CoS values to a queue and to a threshold ID. Use the **no** form of this command to return to the default setting.

```
mls qos srr-queue input cos-map queue queue-id {cos1...cos8 | threshold threshold-id
cos1...cos8}
```

```
no mls qos srr-queue input cos-map
```

Syntax Description		
queue <i>queue-id</i>	Specify a queue number. For <i>queue-id</i> , the range is 1 to 2.	
<i>cos1...cos8</i>	Map CoS values to an ingress queue. For <i>cos1...cos8</i> , enter up to eight values, and separate each value with a space. The range is 0 to 7.	
threshold <i>threshold-id</i> <i>cos1...cos8</i>	Map CoS values to a queue threshold ID. For <i>threshold-id</i> , the range is 1 to 3. For <i>cos1...cos8</i> , enter up to eight values, and separate each value with a space. The range is 0 to 7.	

Defaults

Table 2-10 shows the default CoS input queue threshold map:

Table 2-10 Default CoS Input Queue Threshold Map

CoS Value	Queue ID - Threshold ID
0–4	1 - 1
5	2 - 1
6, 7	1 - 1

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The CoS assigned at the ingress port selects an ingress queue and a threshold.

The drop-threshold percentage for threshold 3 is predefined. It is set to the queue-full state. You can assign two weighted tail-drop (WTD) threshold percentages to an ingress queue by using the **mls qos srr-queue input threshold** global configuration command.

You can map each CoS value to a different queue and threshold combination, allowing the frame to follow different behavior.

Examples

This example shows how to map CoS values 0 to 3 to ingress queue 1 and to threshold ID 1 with a drop threshold of 50 percent. It maps CoS values 4 and 5 to ingress queue 1 and to threshold ID 2 with a drop threshold of 70 percent:

```
Switch(config)# mls qos srr-queue input cos-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos srr-queue input cos-map queue 1 threshold 2 4 5
Switch(config)# mls qos srr-queue input threshold 1 50 70
```

You can verify your settings by entering the **show mls qos maps** privileged EXEC command.

Related Commands

Command	Description
mls qos srr-queue input bandwidth	Assigns shaped round robin (SRR) weights to an ingress queue.
mls qos srr-queue input buffers	Allocates the buffers between the ingress queues.
mls qos srr-queue input dscp-map	Maps Differentiated Services Code Point (DSCP) values to an ingress queue or maps DSCP values to a queue and to a threshold ID.
mls qos srr-queue input priority-queue	Configures the ingress priority queue and guarantees bandwidth.
mls qos srr-queue input threshold	Assigns WTD threshold percentages to an ingress queue.
show mls qos maps	Displays quality of service (QoS) mapping information.

mls qos srr-queue input dscp-map

Use the **mls qos srr-queue input dscp-map** global configuration command to map Differentiated Services Code Point (DSCP) values to an ingress queue or to map DSCP values to a queue and to a threshold ID. Use the **no** form of this command to return to the default setting.

```
mls qos srr-queue input dscp-map queue queue-id {dscp1...dscp8 | threshold threshold-id
dscp1...dscp8}
```

```
no mls qos srr-queue input dscp-map
```

Syntax Description		
queue <i>queue-id</i>	Specify a queue number. For <i>queue-id</i> , the range is 1 to 2.	
<i>dscp1...dscp8</i>	Map DSCP values to an ingress queue. For <i>dscp1...dscp8</i> , enter up to eight values, and separate each value with a space. The range is 0 to 63.	
threshold <i>threshold-id</i> <i>dscp1...dscp8</i>	Map DSCP values to a queue threshold ID. For <i>threshold-id</i> , the range is 1 to 3. For <i>dscp1...dscp8</i> , enter up to eight values, and separate each value with a space. The range is 0 to 63.	

Defaults

Table 2-11 shows the default DSCP input queue threshold map:

Table 2-11 Default DSCP Input Queue Threshold Map

DSCP Value	Queue ID - Threshold ID
0–39	1 - 1
40–47	2 - 1
48–63	1 - 1

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The DSCP assigned at the ingress port selects an ingress queue and a threshold.

The drop-threshold percentage for threshold 3 is predefined. It is set to the queue-full state. You can assign two weighted tail-drop (WTD) threshold percentages to an ingress queue by using the **mls qos srr-queue input threshold** global configuration command.

You can map each DSCP value to a different queue and threshold combination, allowing the frame to follow different behavior.

You can map up to eight DSCP values per command.

Examples

This example shows how to map DSCP values 0 to 6 to ingress queue 1 and to threshold 1 with a drop threshold of 50 percent. It maps DSCP values 20 to 26 to ingress queue 1 and to threshold 2 with a drop threshold of 70 percent.

```
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 1 0 1 2 3 4 5 6
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 20 21 22 23 24 25 26
Switch(config)# mls qos srr-queue input threshold 1 50 70
```

You can verify your settings by entering the **show mls qos maps** privileged EXEC command.

Related Commands

Command	Description
mls qos srr-queue input bandwidth	Assigns shaped round robin (SRR) weights to an ingress queue.
mls qos srr-queue input buffers	Allocates the buffers between the ingress queues.
mls qos srr-queue input cos-map	Maps class of service (CoS) values to an ingress queue or maps CoS values to a queue and to threshold ID.
mls qos srr-queue input priority-queue	Configures the ingress priority queue and guarantees bandwidth.
mls qos srr-queue input threshold	Assigns WTD threshold percentages to an ingress queue.
show mls qos maps	Displays quality of service (QoS) mapping information.

mls qos srr-queue input priority-queue

Use the **mls qos srr-queue input priority-queue** global configuration command to configure the ingress priority queue and to guarantee bandwidth on the internal ring if the ring is congested. Use the **no** form of this command to return to the default setting.

mls qos srr-queue input priority-queue *queue-id* **bandwidth** *weight*

no mls qos srr-queue input priority-queue *queue-id*

Syntax Description

<i>queue-id</i>	Ingress queue ID. The range is 1 to 2.
bandwidth <i>weight</i>	Bandwidth percentage of the internal ring. The range is 0 to 40.

Defaults

The priority queue is queue 2, and 10 percent of the bandwidth is allocated to it.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

You should use the priority queue only for traffic that needs to be expedited (for example, voice traffic, which needs minimum delay and jitter).

The priority queue is guaranteed part of the bandwidth on the internal ring, which reduces the delay and jitter under heavy network traffic on an oversubscribed ring (when there is more traffic than the backplane can carry, and the queues are full and dropping frames).

Shaped round robin (SRR) services the priority queue for its configured weight as specified by the **bandwidth** keyword in the **mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight* global configuration command. Then SRR shares the remaining bandwidth with both ingress queues and services them as specified by the weights configured with the **mls qos srr-queue input bandwidth** *weight1 weight2* global configuration command.

To disable priority queueing, set the bandwidth weight to 0, for example, **mls qos srr-queue input priority-queue** *queue-id* **bandwidth** 0.

Examples

This example shows how to assign the ingress bandwidths for the queues. Queue 1 is the priority queue with 10 percent of the bandwidth allocated to it. The bandwidth ratio allocated to queues 1 and 2 is 4/(4+4). SRR services queue 1 (the priority queue) first for its configured 10 percent bandwidth. Then SRR equally shares the remaining 90 percent of the bandwidth between queues 1 and 2 by allocating 45 percent to each queue.

```
Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config)# mls qos srr-queue input bandwidth 4 4
```

You can verify your settings by entering the **show mls qos interface** *[interface-id]* **queueing** or the **show mls qos input-queue** privileged EXEC command.

Related Commands	Command	Description
	mls qos srr-queue input bandwidth	Assigns SRR weights to an ingress queue.
	mls qos srr-queue input buffers	Allocates the buffers between the ingress queues.
	mls qos srr-queue input cos-map	Maps class of service (CoS) values to an ingress queue or maps CoS values to a queue and to a threshold ID.
	mls qos srr-queue input dscp-map	Maps Differentiated Services Code Point (DSCP) values to an ingress queue or maps DSCP values to a queue and to a threshold ID.
	mls qos srr-queue input threshold	Assigns weighted tail-drop (WTD) threshold percentages to an ingress queue.
	show mls qos input-queue	Displays ingress queue settings.
	show mls qos interface queueing	Displays queueing strategy information.

mls qos srr-queue input threshold

Use the **mls qos srr-queue input threshold** global configuration command to assign weighted tail-drop (WTD) threshold percentages to an ingress queue. Use the **no** form of this command to return to the default setting.

mls qos srr-queue input threshold queue-id threshold-percentage1 threshold-percentage2

no mls qos srr-queue input threshold queue-id

Syntax Description

<i>queue-id</i>	ID of the ingress queue. The range is 1 to 2.
<i>threshold-percentage1</i> <i>threshold-percentage2</i>	Two WTD threshold percentage values. Each threshold value is a percentage of the total number of queue descriptors allocated for the queue. Separate each value with a space. The range is 1 to 100.

Defaults

When quality of service (QoS) is enabled, WTD is enabled.
The two WTD thresholds are set to 100 percent.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

QoS uses the CoS-to-threshold map or the DSCP-to-threshold map to control which class of service (CoS) or Differentiated Services Code Point (DSCP) values are mapped to threshold 1 and to threshold 2. If threshold 1 is exceeded, packets with CoS or DSCP values assigned to this threshold are dropped until the threshold is no longer exceeded. However, packets assigned to threshold 2 continue to be queued and sent as long as the second threshold is not exceeded.

Each queue has two configurable (explicit) drop threshold and one preset (implicit) drop threshold (full).

You configure the CoS-to-threshold map by using the **mls qos srr-queue input cos-map** global configuration command. You configure the DSCP-to-threshold map by using the **mls qos srr-queue input dscp-map** global configuration command.

Examples

This example shows how to configure the tail-drop thresholds for the two queues. The queue 1 thresholds are 50 percent and 100 percent, and the queue 2 thresholds are 70 percent and 100 percent.

```
Switch(config)# mls qos srr-queue input threshold 1 50 100
Switch(config)# mls qos srr-queue input threshold 2 70 100
```

You can verify your settings by entering the **show mls qos interface [interface-id] buffers** or the **show mls qos input-queue** privileged EXEC command.

Related Commands	Command	Description
	mls qos srr-queue input bandwidth	Assigns shaped round robin (SRR) weights to an ingress queue.
	mls qos srr-queue input buffers	Allocates the buffers between the ingress queues.
	mls qos srr-queue input cos-map	Maps CoS values to an ingress queue or maps CoS values to a queue and to a threshold ID.
	mls qos srr-queue input dscp-map	Maps DSCP values to an ingress queue or maps DSCP values to a queue and to a threshold ID.
	mls qos srr-queue input priority-queue	Configures the ingress priority queue and guarantees bandwidth.
	show mls qos input-queue	Displays ingress queue settings.
	show mls qos interface buffers	Displays buffer allocation information.

mls qos srr-queue output cos-map

Use the **mls qos srr-queue output cos-map** global configuration command to map class of service (CoS) values to an egress queue or to map CoS values to a queue and to a threshold ID. Use the **no** form of this command to return to the default setting.

```
mls qos srr-queue output cos-map queue queue-id {cos1...cos8 | threshold threshold-id
cos1...cos8}
```

```
no mls qos srr-queue output cos-map
```

Syntax Description

queue <i>queue-id</i>	Specify a queue number. For <i>queue-id</i> , the range is 1 to 4.
<i>cos1...cos8</i>	Map CoS values to an egress queue. For <i>cos1...cos8</i> , enter up to eight values, and separate each value with a space. The range is 0 to 7.
threshold <i>threshold-id</i> <i>cos1...cos8</i>	Map CoS values to a queue threshold ID. For <i>threshold-id</i> , the range is 1 to 3. For <i>cos1...cos8</i> , enter up to eight values, and separate each value with a space. The range is 0 to 7.

Defaults

Table 2-12 shows the default CoS output queue threshold map:

Table 2-12 Default CoS Output Queue Threshold Map

CoS Value	Queue ID - Threshold ID
0, 1	2 - 1
2, 3	3 - 1
4	4 - 1
5	1 -1
6, 7	4 - 1

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The drop-threshold percentage for threshold 3 is predefined. It is set to the queue-full state.

**Note**

The egress queue-set default settings are suitable for most situations. You should change them only when you have a thorough understanding of the queues and if these settings do not meet your quality of service (QoS) solution.

You can assign two weighted tail-drop (WTD) threshold percentages to an egress queue-set by using the **mls qos queue-set output *qset-id* threshold** global configuration command.

You can map each CoS value to a different queue and threshold combination, allowing the frame to follow different behavior.

Examples

This example shows how to map a port to queue-set 1. It maps CoS values 0 to 3 to egress queue 1 and to threshold ID 1. It configures the drop thresholds for queue 1 to 50 and 70 percent of the allocated memory, guarantees (reserves) 100 percent of the allocated memory, and configures 200 percent as the maximum memory that this queue can have before packets are dropped.

```
Switch(config)# mls qos srr-queue output cos-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos queue-set output 1 threshold 1 50 70 100 200
Switch(config)# interface fastethernet1/0/1
Switch(config-if)# queue-set 1
```

You can verify your settings by entering the **show mls qos maps**, the **show mls qos interface *[interface-id]* buffers**, or the **show mls qos queue-set** privileged EXEC command.

Related Commands

Command	Description
mls qos srr-queue output dscp-map	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
mls qos queue-set output threshold	Configures the WTD thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
queue-set	Maps a port to a queue-set.
show mls qos interface buffers	Displays QoS information.
show mls qos maps	Displays buffer allocation information.
show mls qos queue-set	Displays settings for the queue-set.

mls qos srr-queue output cpu-queue

Use the **mls qos srr-queue output cpu queue** global configuration command to assign CPU-generated control plane packets to an egress queue and to specify the threshold values. Use the **no** form of this command to return to the default setting.

mls qos srr-queue output cpu queue *queue-id* **threshold** *threshold-id*

no mls qos srr-queue output cpu queue *queue -d* **threshold** *threshold-id*

Syntax Description

queue <i>queue-id</i>	Specify an egress queue and ID. The range is 1 to 4.
threshold <i>threshold-id</i>	Specify a threshold value and ID. The range is 1 to 3.

Defaults

The default egress queue value is 2.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use this command to specify an egress queue and a threshold ID for CPU-generated traffic.

You can assign each packet that flows through the switch to a queue and to a threshold. Specifically, you map Differentiated Services Code Value (DSCP) or Class of Service (CoS) values to an egress queue-set and map DSCP or CoS values to a threshold ID. You use the **mls qos srr-queue output dscp-map queue** *queue-id* {*dscp1...dscp8* | **threshold** *threshold-id* *dscp1...dscp8*} or the **mls qos srr-queue output cos-map queue** *queue-id* {*cos1...cos8* | **threshold** *threshold-id* *cos1...cos8*} global configuration command. When you mark a CPU-generated control plane packet with a DSCP or CoS value, you can map traffic to any of the four egress queues.

Examples

This example shows how to specify an egress queue for CPU-generated traffic. In this example, the traffic is sent from queue 2 and has a threshold ID of 1.

```
Switch(config)# mls qos srr-queue output cpu queue 2 threshold 1
Switch(config)# cpu traffic qos dscp 20
```

Note that threshold 3 specifically applies to CPU-generated traffic. For example: If you explicitly issue the **mls qos srr-queue output cpu queue 3 threshold 3** command, then traffic is always sent through queue 3 regardless of the **dscp-map** or **cpu traffic qos** marking settings.

You can verify your settings by entering the **show mls qos maps**, the **show mls qos interface** [*interface-id*] **buffers**, or the **show mls qos queue-set** privileged EXEC commands.

Related Commands	Command	Description
	cpu traffic qos	Configures the QoS packet marking for CPU-generated traffic.
	mls qos srr-queue output cos-map	Maps class of service (CoS) values to an egress queue or maps CoS values to a queue and to a threshold ID.
	mls qos queue-set output threshold	Configures the WTD thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
	mls qos srr-queue output dscp-map	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
	queue-set	Maps a port to a queue-set.
	show mls qos input-queue	Display QoS settings for the ingress queue.
	show mls qos maps	Displays QoS mapping information.
	show mls qos queue-set	Display settings for the queue-set.

mls qos srr-queue output dscp-map

Use the **mls qos srr-queue output dscp-map** global configuration command to map Differentiated Services Code Point (DSCP) values to an egress queue or to map DSCP values to a queue and to a threshold ID. Use the **no** form of this command to return to the default setting.

```
mls qos srr-queue output dscp-map queue queue-id {dscp1...dscp8 | threshold threshold-id
dscp1...dscp8}
```

```
no mls qos srr-queue output dscp-map
```

Syntax Description	
queue <i>queue-id</i>	Specify a queue number. For <i>queue-id</i> , the range is 1 to 4.
<i>dscp1...dscp8</i>	Map DSCP values to an egress queue. For <i>dscp1...dscp8</i> , enter up to eight values, and separate each value with a space. The range is 0 to 63.
threshold <i>threshold-id</i> <i>dscp1...dscp8</i>	Map DSCP values to a queue threshold ID. For <i>threshold-id</i> , the range is 1 to 3. For <i>dscp1...dscp8</i> , enter up to eight values, and separate each value with a space. The range is 0 to 63.

Defaults

Table 2-13 shows the default DSCP output queue threshold map:

Table 2-13 Default DSCP Output Queue Threshold Map

DSCP Value	Queue ID - Threshold ID
0–15	2 - 1
16–31	3 - 1
32–39	4 - 1
40–47	1 -1
48–63	4 - 1

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The drop-threshold percentage for threshold 3 is predefined. It is set to the queue-full state.

**Note**

The egress queue-set default settings are suitable for most situations. You should change them only when you have a thorough understanding of the queues and if these settings do not meet your quality of service (QoS) solution.

You can assign two weighted tail-drop (WTD) threshold percentages to an egress queue-set by using the **mls qos queue-set output *qset-id* threshold** global configuration command.

You can map each DSCP value to a different queue and threshold combination, allowing the frame to follow different behavior.

You can map up to eight DSCP values per command.

Examples

This example shows how to map a port to queue-set 1. It maps DSCP values 0 to 3 to egress queue 1 and to threshold ID 1. It configures the drop thresholds for queue 1 to 50 and 70 percent of the allocated memory, guarantees (reserves) 100 percent of the allocated memory, and configures 200 percent as the maximum memory that this queue can have before packets are dropped.

```
Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos queue-set output 1 threshold 1 50 70 100 200
Switch(config)# interface fastethernet1/0/1
Switch(config-if)# queue-set 1
```

You can verify your settings by entering the **show mls qos maps**, the **show mls qos interface *[interface-id]* buffers**, or the **show mls qos queue-set** privileged EXEC command.

Related Commands

Command	Description
mls qos srr-queue output cos-map	Maps class of service (CoS) values to an egress queue or maps CoS values to a queue and to a threshold ID.
mls qos queue-set output threshold	Configures the WTD thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
queue-set	Maps a port to a queue-set.
show mls qos interface buffers	Displays buffer allocation information.
show mls qos maps	Displays QoS mapping information.
show mls qos queue-set	Displays settings for the queue-set.

mls qos trust

Use the **mls qos trust** interface configuration command to configure the port trust state. Ingress traffic can be trusted, and classification is performed by examining the packet Differentiated Services Code Point (DSCP), class of service (CoS), or IP-precedence field. Use the **no** form of this command to return a port to its untrusted state.

mls qos trust [**cos** | **device cisco-phone** | **dscp** | **ip-precedence**]

no mls qos trust [**cos** | **device** | **dscp** | **ip-precedence**]

Syntax Description	
cos	(Optional) Classify an ingress packet by using the packet CoS value. For an untagged packet, use the port default CoS value.
device cisco-phone	(Optional) Classify ingress packets by trusting the value sent from the Cisco IP phone (trusted boundary).
dscp	(Optional) Classify an ingress packet by using the packet DSCP value (most significant 6 bits of 8-bit service-type field). For a non-IP packet, the packet CoS is used if the packet is tagged. For an untagged packet, the default port CoS value is used.
ip-precedence	(Optional) Classify an ingress packet by using the packet IP-precedence value (most significant 3 bits of 8-bit service-type field). For a non-IP packet, the packet CoS is used if the packet is tagged. For an untagged packet, the port default CoS value is used.

Defaults The port is not trusted. If no keyword is specified when the command is entered, the default is **dscp**.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines Packets entering a quality of service (QoS) domain are classified at the edge of the domain. When the packets are classified at the edge, the switch port within the QoS domain can be configured to one of the trusted states because there is no need to classify the packets at every switch within the domain. Use this command to specify whether the port is trusted and which fields of the packet to use to classify traffic.

When a port is configured with trust DSCP or trust IP precedence and the inbound packet is a non-IP packet, the CoS-to-DSCP map is used to derive the corresponding DSCP value from the CoS value. The CoS can be the packet CoS for trunk ports or the port default CoS for nontrunk ports.

If the DSCP is trusted, the DSCP field of the IP packet is not modified. However, it is still possible that the CoS value of the packet is modified (according to DSCP-to-CoS map).

If the CoS is trusted, the CoS field of the packet is not modified, but the DSCP can be modified (according to the CoS-to-DSCP map) if the packet is an IP packet.

The trusted boundary feature prevents security problems if users disconnect their PCs from networked Cisco IP phones and connect them to the switch port to take advantage of trusted CoS settings. You must globally enable the Cisco Discovery Protocol (CDP) on the switch and on the port connected to the Cisco IP phone. If the phone is not detected, trusted boundary disables the trusted setting on the switch port and prevents misuse of a high-priority queue. If you configure the trust setting for DSCP or IP precedence, the DSCP or IP precedence values in the inbound packets are trusted. If you configure the **mls qos cos override** interface configuration command on the switch port connected to the Cisco IP phone, the switch overrides the CoS of the inbound voice and data packets and assigns the default CoS value to them.

For an inter-QoS domain boundary, you can configure the port to the DSCP-trusted state and apply the DSCP-to-DSCP-mutation map if the DSCP values are different between the QoS domains.

Classification using a port trust state (for example, **mls qos trust [cos | dscp | ip-precedence]** and a policy map (for example, **service-policy input policy-map-name**) are mutually exclusive. The last one configured overwrites the previous configuration.

When port trust policies are used with 802.1Q tunneling, all ports sharing the same tunnel VLAN must be configured with the same trust policy, and the ports involved must use the same DSCP-to-DSCP mutation map. For more information, see the “[mls qos dscp-mutation](#)” section on page 2-248 and the “[mls qos map](#)” section on page 2-252.

For 802.1Q tunnels, the switch processes inbound traffic on a standard port according to the trusted setting applied to this port. The switch configures the inner and outer tags for packets sent over the enhanced-services (ES) trunk port as follows:

- If no trust state is configured on a standard port, the switch does not copy the inner CoS value to the outer CoS value.
- If the trust CoS state is configured on a standard port, the switch classifies inbound traffic by using the packet CoS value. For an untagged packet, the switch uses the CoS value configured on that port. If no CoS value is configured, the switch uses the default CoS value (0). The switch copies the inner CoS value to the outer CoS value and sends the packet to an ES port.
- If the trust DSCP state is configured on the standard port, the switch classifies inbound traffic by using the packet DSCP value if the packet is an IP packet. For a non-IP packet that is tagged, the switch uses the packet CoS value to generate a DSCP value through the CoS-to-DSCP map. For a non-IP packet that is untagged, the switch uses the port CoS value to generate the DSCP from the CoS-to-DSCP map. The switch configures the outer CoS value from the DSCP-to-CoS map, does not modify the inner CoS value, and sends the packet to an ES port.

For an IP packet, the switch modifies the DSCP value in the packet if there is a DSCP-to-DSCP mutation map configured on the standard port. The switch uses the mutated DSCP value to configure the outer CoS value from the DSCP-to-CoS map and sends the packet to an ES port.

- If the trust IP precedence state is configured on the standard port, the switch classifies inbound traffic by using the packet IP precedence value. For a non-IP packet, the switch uses the packet CoS value if the packet is tagged. For an untagged packet, the switch uses the port CoS value and then generates the DSCP value by using the CoS-to-DSCP map. The switch converts the generated DSCP value from the DSCP-to-CoS map and uses it as the outer CoS value in the packet. The switch does not modify the inner CoS value in the packet and sends the packet to an ES port.
- If the CoS override state is configured on the standard port, the switch overrides the previously configured port trust state and applies the CoS value configured on the port to all inbound traffic. The switch copies the port CoS value to the outer CoS value, does not modify the inner CoS value, and sends the packet to an ES port.

**Note**

When a trust policy and a hierarchical ingress policy are both configured on an ES port, the actions specified in the service policy are processed before the trust policy is applied.

Examples

This example shows how to configure a port to trust the IP precedence field in the inbound packet:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mls qos trust ip-precedence
```

This example shows how to specify that the Cisco IP phone connected on a port is a trusted device:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mls qos trust device cisco-phone
```

You can verify your settings by entering the **show mls qos interface** privileged EXEC command.

Related Commands

Command	Description
mls qos cos	Defines the default CoS value of a port or assigns the default CoS to all inbound packets on the port.
mls qos dscp-mutation	Applies a DSCP-to DSCP-mutation map to a DSCP-trusted port.
mls qos map	Defines the CoS-to-DSCP map, the DSCP-to-CoS map, the DSCP-to-DSCP-mutation map, the IP-precedence-to-DSCP map, and the policed-DSCP map.
show mls qos interface	Displays QoS information at the port level.

mls qos vlan-based

Use the **mls qos vlan-based** interface configuration command to enable VLAN-based quality of service (QoS) on the physical port. Use the **no** form of this command to disable this feature.

mls qos vlan-based

no mls qos vlan-based

Syntax Description

There are no arguments or keywords.

Defaults

VLAN-based QoS is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(25)EY	This command was introduced.

Usage Guidelines

Before attaching a hierarchical dual-level policy map to a switch virtual interface (SVI), use the **mls qos vlan-based** interface configuration command on a physical port if the port is to be specified in the secondary interface level of the dual-level policy map.

When you configure dual-level policing, the dual-level policy map is attached to the SVI and affects all traffic belonging to the VLAN. The individual policer in the interface-level traffic classification only affects the physical ports specified for that classification.

For detailed instructions about configuring dual-level policy maps, see the “Classifying, Policing, and Marking Traffic by Using Dual-Level Policy Maps” section in the software configuration guide for this release.

Examples

This example shows how to enable VLAN-based policing on a physical port:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mls qos vlan-based
```

You can verify your settings by entering the **show mls qos interface** privileged EXEC command.

Related Commands

Command	Description
show mls qos interface	Displays QoS information.

monitor session

Use the **monitor session** global configuration command to start a new Switched Port Analyzer (SPAN) session or Remote SPAN (RSPAN) source or destination session, to enable ingress traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance), to add or delete interfaces or VLANs to or from an existing SPAN or RSPAN session, and to limit (filter) SPAN source traffic to specific VLANs. Use the **no** form of this command to remove the SPAN or RSPAN session or to remove source or destination interfaces or filters from the SPAN or RSPAN session. For destination interfaces, the **encapsulation replicate** keywords are ignored with the **no** form of the command.

```
monitor session session_number destination {interface interface-id [, | -] [encapsulation
replicate] [ingress {dot1q vlan vlan-id | isl | untagged vlan vlan-id | vlan vlan-id}] } | {remote
vlan vlan-id}
```

```
monitor session session_number filter vlan vlan-id [, | -]
```

```
monitor session session_number source {interface interface-id [, | -] [both | rx | tx]} | {remote
vlan vlan-id} | {vlan vlan-id [, | -] [both | rx | tx]}
```

```
no monitor session {session_number | all | local | remote}
```

```
no monitor session session_number destination {interface interface-id [, | -] [encapsulation
replicate] [ingress {dot1q vlan vlan-id | isl | untagged vlan vlan-id | 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]} | {remote
vlan vlan-id} | {vlan vlan-id [, | -] [both | rx | tx]}
```

Syntax Description

<i>session_number</i>	Specify the session number identified with the SPAN or RSPAN session. The range is 1 to 66.
destination	Specify the SPAN or RSPAN destination. A destination must be a physical port.
interface <i>interface-id</i>	Specify the destination or source interface for a SPAN or RSPAN session. Valid interfaces are physical ports. For source interface , port channel is also a valid interface type, and the valid range is 1 to 12.
encapsulation replicate	(Optional) Specify that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged). Note 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.
ingress	(Optional) Enable ingress traffic forwarding.
dot1q vlan <i>vlan-id</i>	Specify ingress forwarding using 802.1Q encapsulation with the specified VLAN as the default VLAN for ingress traffic.
isl	Specify ingress forwarding using ISL encapsulation.
untagged vlan <i>vlan-id</i>	Specify ingress forwarding using untagged encapsulation with the specified VLAN as the default VLAN for ingress traffic

vlan <i>vlan-id</i>	When used with only the ingress keyword, set default VLAN for ingress traffic.
remote vlan <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. Note The RSPAN VLAN cannot be VLAN 1 (the default VLAN) or VLAN IDs 1002 to 1005 (reserved for Token Ring and FDDI VLANs).
,	(Optional) Specify a series of interfaces or VLANs, or separate a range of interfaces or VLANs from a previous range. Enter a space before and after the comma.
-	(Optional) Specify a range of interfaces or VLANs. Enter a space before and after the hyphen.
filter vlan <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.
source	Specify the SPAN or RSPAN source. A source can be a physical port, a port channel, or a VLAN.
both, rx, tx	(Optional) Specify the traffic direction to monitor. If you do not specify a traffic direction, the source interface sends both transmitted and received traffic.
source vlan <i>vlan-id</i>	Specify the SPAN source interface as a VLAN ID. The range is 1 to 4094.
all, local, remote	Specify all , local , or remote with the no monitor session command to clear all SPAN and RSPAN, all local SPAN, or all RSPAN sessions.

Defaults

No monitor sessions are configured.

On a source interface, the default is to monitor both received and transmitted traffic.

On a trunk interface used as a source port, all VLANs are monitored.

If **encapsulation replicate** is not specified on a local SPAN destination port, packets are sent in native form with no encapsulation tag.

Ingress forwarding is disabled on destination ports.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	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.

An enhanced services (ES) port cannot be a source port for a monitoring session.

You can set a combined maximum of two local SPAN sessions and RSPAN source sessions. You can have a total of 66 SPAN and RSPAN sessions on a switch.

You can have a maximum of 64 destination ports on a switch.

Each session can include multiple ingress or egress source ports or VLANs, but you cannot combine source ports and source VLANs in a single session. Each session can include multiple destination ports.

When you use VLAN-based SPAN (VSPAN) to analyze network traffic in a VLAN or set of VLANs, all active ports in the source VLANs become source ports for the SPAN or RSPAN session. Trunk ports are included as source ports for VSPAN, and only packets with the monitored VLAN ID are sent to the destination port.

You can monitor traffic on a single port or VLAN or on a series or range of ports or VLANs. You select a series or range of interfaces or VLANs by using the [, | -] options.

If you specify a series of VLANs or interfaces, you must enter a space before and after the comma. If you specify a range of VLANs or interfaces, you must enter a space before and after the hyphen (-).

EtherChannel ports cannot be configured as SPAN or RSPAN destination ports. A physical port that is a member of an EtherChannel group can be used as a destination port, but it cannot participate in the EtherChannel group while it is as a SPAN destination.

You can monitor individual ports while they participate in an EtherChannel, or you can monitor the entire EtherChannel bundle by specifying the **port-channel** number as the RSPAN source interface.

A port used as a destination port cannot be a SPAN or RSPAN source, nor can a port be a destination port for more than one session at a time.

You can enable 802.1x on a port that is a SPAN or RSPAN destination port; however, 802.1x is disabled until the port is removed as a SPAN destination. (If 802.1x is not available on the port, the switch returns an error message.) You can enable 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**, **isl**, 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**, **isl**, or **untagged**.

Examples

This example shows how to create a local SPAN session 1 to monitor both sent and received traffic on source port Gigabit Ethernet 1 to destination port Gigabit Ethernet 2:

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
```

This example shows how to delete a destination port from an existing local SPAN session:

```
Switch(config)# no monitor session 2 destination gigabitethernet1/0/2
```

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 fastethernet1/0/10 , fastethernet1/0/12
Switch(config)# monitor session 1 source interface fastethernet1/0/2 rx
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 fastethernet1/0/10
```

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that supports 802.1Q encapsulation. Egress traffic replicates the source; ingress traffic uses 802.1Q encapsulation.

```
Switch(config)# monitor session 2 destination interface fastethernet1/0/5 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 fastethernet1/0/5 ingress untagged
vlan 5
```

You can verify your settings by entering the **show monitor** privileged EXEC command. You can view 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
remote-span	Configures an RSPAN VLAN in vlan configuration mode.
show monitor	Displays SPAN and RSPAN session information.
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.

mpls l2transport route

Use the **mpls l2transport route** interface configuration command at a customer edge (CE) standard port, a provider-edge customer-located equipment (PE-CLE) enhanced-services (ES) port, or a VLAN interface to enable forwarding Layer 2 packets over a specified point-to-point virtual connection (VC) by using Ethernet over multiprotocol label switching (EoMPLS). Enter the command at the local and remote edge devices. Use the **no** form of this command on both provider edge devices to delete the VC.

mpls l2transport route *destination vc-id*

no mpls l2transport route

Syntax Description

<i>destination</i>	The destination label distribution protocol (LDP) IP address of the remote provider edge device. The IP address cannot be an IP address on the route on which the command is entered.
<i>vc-id</i>	Assign a virtual connection identifier (VC ID) to the virtual connection between the two peer provider edge devices. The range is from 1 to 4294967295.

Defaults

No point-to-point connection is established.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

A multiprotocol label switching (MPLS) VC runs across an MPLS cloud to connect Ethernet interfaces on a provider edge device at each edge of the service provider network. The command must be entered on the connecting interface on the device at each edge of the service provider network to establish a bidirectional virtual connection, which is made of two unidirectional label-switched paths (LSPs). A VC is not established if not properly defined from both ends.

For the *destination* parameter, specify the LDP IP address of the other PE edge device; do not specify the IP address of the device on which you are entering the command.

The *vc-id* must be unique for each pair of provider edge devices. Therefore, in large networks, you should track the VC ID assignments to ensure that a VC ID is not assigned more than once.



Note

EoMPLS operation between PE devices requires an LDP session between the two devices. For information about LDP configuration and commands, see the [MPLS Label Distribution Protocol](#) feature module. See also the [Multiprotocol Label Switching on Cisco Routers](#) feature module.

Examples

This example shows how to establish an Ethernet over MPLS (EoMPLS) tunnel between the PE1 VLAN 3 interface and the PE2 VLAN 4 interface. PE1 has IP address 10.0.0.1/32 that PE2 discovers through routing, and PE2 has IP address 20.0.0.1/32 that PE1 discovers through routing.

At the PE1 interface:

```
Switch(config)# interface vlan 3
Switch(config-if)# mpls l2transport route 20.0.0.1 123
```

At the PE2 interface:

```
Switch(config)# interface vlan 4
Switch(config-if)# mpls l2transport route 10.0.0.1 123
```

You can verify your setting by entering the **show mpls l2transport vc** privileged EXEC command.

Related Commands

Command	Description
show mpls l2transport vc	Displays information about the EoMPLS VCs that have been enabled to route Layer 2 packets on a device.

mpls ldp holdtime

Use the **mpls ldp holdtime** global configuration command to change the time for which a Label Distribution Protocol (LDP) session is maintained in the absence of LDP messages from the session peer. Use the **no** form of the command to return to the default.

mpls ldp holdtime {*seconds* | **infinite**}

no mpls holdtime

Syntax Description	<i>seconds</i>	The time interval in seconds that an LDP session is maintained in the absence of LDP messages from the session peer. The range is from 15 to 2147483 seconds. The default is 180 seconds.
	infinite	Configure the switch to ignore the LDP session holdtime and maintain the session until it is manually ended.

Defaults The default holdtime for an LDP session is 180 seconds.

Command Modes Global configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines When an LDP session is established between two label switch routers (LSRs), the holdtime used for the session is the lower of the values configured on the two LSRs.



Note

For information about LDP configuration and commands, see the [MPLS Label Distribution Protocol](#) feature module.

Examples This example shows how to set the holdtime for LDP sessions for 30 seconds:

```
Switch(config)# mpls ldp holdtime 30
```

You can verify your setting by entering the **show mpls ldp parameters** privileged EXEC command.

Related Commands	Command	Description
	show mpls ldp parameters	Displays the current LDP parameters.

mpls mtu

Use the **mpls mtu** interface configuration command on an enhanced-services (ES) port to set the per-interface maximum transmission unit (MTU) for multiprotocol label switching (MPLS) labeled packets. Use the **no** form of this command to return to the default MTU setting.

mpls mtu *bytes*

no mpls mtu

Syntax Description	<i>bytes</i>	The MTU value in bytes. The range is from 64 to 65536 bytes.

Defaults	The system MTU is used if no MPLS MTU is configured.	

Command Modes	Interface configuration	

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	If a labeled or nonlabeled IPv4 packet exceeds the MPLS MTU size for the interface, the packet is dropped.	
	All devices on a physical medium must have the same MPLS MTU value for MPLS to operate between the devices.	
	If the mpls mtu bytes command is not used to configure an interface MTU, the MTU for labeled packets is the system MTU for the interface.	
	Because labeling a packet makes it larger, we recommend making the system MTU the same size as the MPLS MTU to prevent dropping of labeled packets. We recommend using the system mtu routing global configuration command to set a lower MTU value for the routing protocols.	
	Using the mpls mtu bytes command to change the MPLS MTU does not change the interface MTU.	



Note

See the [Multiprotocol Label Switching on Cisco Routers](#) feature module for more information about configuring MPLS.

Examples	This example shows how to set the maximum labeled packet size for a port to 3500 bytes: Switch(config)# interface gigabitethernet1/1/1 Switch(config-if)# mpls mtu 3500	

Related Commands	Command	Description
	<code>system mtu jumbo</code>	Set the system jumbo frame size (MTU) for Gigabit Ethernet ports. The range is 1500 to 9000 bytes.
	<code>system mtu routing</code>	Set the system MTU for routed ports. The range is 1500 to 1600 bytes.

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, configure the MVR IP multicast address, set the maximum time to wait for a query reply before removing a port from group membership, and to specify the MVR multicast VLAN. Use the **no** form of this command to return to the default settings.

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

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

Syntax Description

group <i>ip-address</i>	Statically configure an MVR group IP multicast address on the switch. Use the no form of this command to remove a statically configured IP multicast address or contiguous addresses or, when no IP address is entered, to remove all statically configured MVR IP multicast addresses.
<i>count</i>	(Optional) Configure multiple contiguous MVR group addresses. The range is 1 to 256; the default is 1.
mode	(Optional) Specify the MVR mode of operation. The default is compatible mode.
compatible	Set MVR mode to provide compatibility with Catalyst 2900 XL and 3500 XL switches. This mode does not allow dynamic membership joins on source ports.
dynamic	Set MVR mode to allow dynamic MVR membership on source ports.
querytime <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 or one-half second. Use the no form of the command to return to the default setting.
vlan <i>vlan-id</i>	(Optional) Specify the VLAN on which MVR multicast data is expected to be received. This is also the VLAN to which all the source ports belong. The range is 1 to 4094; the default is VLAN 1.

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 of or one-half second.

The default multicast VLAN for MVR is VLAN 1.

Command Modes Global configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

MVR can coexist with IGMP snooping on a switch.

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

Examples

This example shows how to enable MVR:

```
Switch(config)# mvr
```

This example shows how to disable MVR:

```
Switch(config)# no 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
```

This example shows how to delete the previously configured ten IP multicast addresses:

```
Switch(config)# no mvr group 228.1.23.1 10
```

This example shows how to delete all previously configured IP multicast addresses:

```
Switch(config)# no mvr group
```

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

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

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

This example shows how to return the maximum query response time to the default setting of one-half second:

```
Switch(config)# no mvr querytime
```

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
mvr (interface configuration)	Configures MVR ports.
show mvr	Displays MVR global parameters or port parameters.
show mvr interface	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.
show mvr members	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 and set the immediate leave feature, and 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 {source | receiver} | vlan vlan-id {[group ip-address][receiver vlan vlan-id]}]
```

Syntax Description	
immediate	(Optional) Enable the Immediate Leave feature of MVR on a port. Use the no mvr immediate command to disable the feature.
type	(Optional) Configure the port as an MVR receiver port or source port. The default port type is neither an MVR source nor receiver port. The no mvr type command resets the port as neither a source or receiver port.
receiver	Configure the port as a subscriber port that can only receive multicast data. Receiver ports cannot belong to the multicast VLAN.
source	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. Note 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).
vlan <i>vlan-id</i>	Specify the mvr vlan for the system.
group <i>ip-address</i>	(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.
receiver vlan <i>vlan-id</i>	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
12.1(14)AX	This command was introduced.
12.2(35)SE	The receiver and <i>vlan-id</i> keywords were added. These are required to configure a trunk port as an MVR receiver port.

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 a 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.

Examples

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

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

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

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# mvr type source
```

This example shows how to remove a port as an MVR port:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no mvr
```

This example shows how to display configured receiver ports and source ports.

```
Switch# show mvr interface
```

Port	Type	Mode	VLAN	Status	Immediate Leave
----	----	----	----	-----	-----
Fa0/2	RECEIVER	Trunk	1	ACTIVE/UP	DISABLED
Fa0/4	RECEIVER	Trunk	1	ACTIVE/UP	DISABLED
Fa0/5	RECEIVER	Trunk	1	ACTIVE/UP	DISABLED
Fa0/5	RECEIVER	Trunk	2	ACTIVE/UP	DISABLED
Fa0/10	SOURCE	Access	10	ACTIVE/UP	DISABLED

Fa0/11	SOURCE	Trunk	10	ACTIVE/UP	ENABLED
Fa0/16	RECEIVER	Trunk	2	ACTIVE/UP	DISABLED
Fa0/18	RECEIVER	Trunk	1	ACTIVE/UP	ENABLED
Fa0/18	RECEIVER	Trunk	2	ACTIVE/UP	ENABLED
Fa0/21	SOURCE	Access	10	ACTIVE/UP	DISABLED
Fa0/24	RECEIVER	Access	4	ACTIVE/DOWN	DISABLED
Gi0/1	RECEIVER	Trunk	1	ACTIVE/UP	DISABLED
Gi0/1	RECEIVER	Trunk	2	ACTIVE/UP	DISABLED
Gi0/2	SOURCE	Access	10	ACTIVE/UP	DISABLED

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

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

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

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no mvr immediate
```

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

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

This example shows how to add a port 5 on VLAN 100 as a static member of IP multicast group 239.1.1.1. In this example, the receiver port is a trunk port:

```
Switch(config)# interface fastethernet0/5
Switch(config-if)# mvr vlan 100 group 239.1.1.1 receiver vlan 201
```

This example shows how to remove this port from membership:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no mvr vlan5 group 228.1.23.4
```

This example shows how to remove this port from all IP multicast groups:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no mvr vlan5 group
```

This example shows the result if you try to add a port to a multicast group and the port is not a receiver port:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# mvr vlan 1 group 230.1.23.4
Interface Gi1/0/2 not configured as a receiver interface
```

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
	mvr (global configuration)	Enables and configures multicast VLAN registration on the switch.
	show mvr	Displays MVR global parameters or port parameters.
	show mvr interface	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.
	show mvr members	Displays all receiver ports that are members of an MVR multicast group.

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.
	domain <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(25)SEG	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-evc)# oam protocol cfm svlan 22 domain Operator
```

Related Commands	Command	Description
	ethernet evc <i>evc-id</i>	Defines an EVC and enters EVC configuration mode.
	ethernet cfm domain	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 inbound packets received from an EtherChannel port. Use the **no** form of this command to return to the default setting.

pagp learn-method { aggregation-port | physical-port }

no pagp learn-method

Syntax Description

aggregation-port	Specify address learning on the logical port-channel. The switch sends packets to the source using any of the ports in the EtherChannel. This setting is the default. With aggregate-port learning, it is not important on which physical port the packet arrives.
physical-port	Specify address learning on the physical port within the EtherChannel. The switch sends packets to the source using the same port in the EtherChannel from which it learned the source address. The other end of the channel uses the same port in the channel for a particular destination MAC or IP address.

Defaults

The default is aggregation-port (logical port channel).

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The learn method must be configured the same at both ends of the link.



Note

The Catalyst 3750 Metro switch supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the command-line interface (CLI). The **pagp learn-method** and the **pagp port-priority** interface configuration commands have no effect on the switch hardware, but they are required for PAGP interoperability with devices that only support address learning by physical ports, such as the Catalyst 1900 switch.

When the link partner to the Catalyst 3750 Metro switch is a physical learner, we recommend that you configure the switch as a physical-port learner by using the **pagp learn-method physical-port** interface configuration command and to set the load-distribution method based on the source MAC address by using the **port-channel load-balance src-mac** global configuration command. Use the **pagp learn-method** interface configuration command only in this situation.

Examples

This example shows how to set the learning method to learn the address on the physical port within the EtherChannel:

```
Switch(config-if)# pagp learn-method physical-port
```

This example shows how to set the learning method to learn the address on the port-channel within the EtherChannel:

```
Switch(config-if)# pagp learn-method aggregation-port
```

You can verify your settings by entering the **show running-config** privileged EXEC command or the **show pagp channel-group-number internal** privileged EXEC command.

Related Commands

Command	Description
pagp port-priority	Selects a port over which all traffic through the EtherChannel is sent.
show pagp	Displays PAgP channel-group information.
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 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
```

Syntax Description	priority	A priority number ranging from 0 to 255.

Defaults	The default is 128.

Command Modes	Interface configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	The physical port with the highest priority that is operational and has membership in the same EtherChannel is the one selected for PAgP transmission.



Note

The switch supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the command-line interface (CLI). The **pagp learn-method** and the **pagp port-priority** interface configuration commands have no effect on the switch hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports, such as the Catalyst 1900 switch.

When the link partner to the switch is a physical learner, we recommend that you configure the switch as a physical-port learner by using the **pagp learn-method physical-port** interface configuration command and to set the load-distribution method based on the source MAC address by using the **port-channel load-balance src-mac** global configuration command. Use the **pagp learn-method** interface configuration command only in this situation.

Examples	This example shows how to set the port priority to 200: <pre>Switch(config-if)# pagp port-priority 200</pre> You can verify your setting by entering the show running-config privileged EXEC command or the show pagp channel-group-number internal privileged EXEC command.

Related Commands	Command	Description
	pagp learn-method	Provides the ability to learn the source address of inbound packets.
	show pagp	Displays PAgP channel-group information.
	show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.

permit

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 | aarp | amber | cos cos | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavr-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 | aarp | amber | cos cos | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavr-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

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

lsap <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.
mop-console	(Optional) Select EtherType DEC-MOP Remote Console.
mop-dump	(Optional) Select EtherType DEC-MOP Dump.
msdos	(Optional) Select EtherType DEC-MSDOS.
mumps	(Optional) Select EtherType DEC-MUMPS.
netbios	(Optional) Select EtherType DEC- Network Basic Input/Output System (NETBIOS).
vines-echo	(Optional) Select EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
vines-ip	(Optional) Select EtherType VINES IP.
xns-ldp	(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 2-14](#).

Table 2-14 IPX Filtering Criteria

IPX Encapsulation Type		
Cisco IOS Name	Novell Name	Filter Criterion
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
12.1(14)AX	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 name 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 name 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
deny	Denies non-IP traffic to be forwarded if conditions are matched.
mac access-list extended	Creates an access list based on MAC addresses for non-IP traffic.
show access-lists	Displays access control lists configured on a switch.

permit (ARP access-list configuration)

Use the **permit** Address Resolution Protocol (ARP) access-list configuration command on the switch stack or on a standalone switch to permit 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 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

request	(Optional) Requests a match for the ARP request. When request is not specified, matching is performed against all ARP packets.
ip	Specify the sender IP address.
any	Accept any IP or MAC address.
host <i>sender-ip</i>	Accept the specified sender IP address.
<i>sender-ip sender-ip-mask</i>	Accept the specified range of sender IP addresses.
mac	Specify the sender MAC address.
host <i>sender-mac</i>	Accept the specified sender MAC address.
<i>sender-mac sender-mac-mask</i>	Accept the specified range of sender MAC addresses.
response ip	Define the IP address values for the ARP responses.
host <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.
mac	Specify the MAC address values for the ARP responses.
host <i>target-mac</i>	(Optional) Accept the specified target MAC address.
<i>target-mac target-mac-mask</i>	(Optional) Accept the specified range of target MAC addresses.
log	(Optional) Log a packet when it matches the ACE. Matches are logged if you also configure the matchlog keyword in the ip arp inspection vlan logging global configuration command.

Defaults

There are no default settings.

Command Modes

ARP access-list configuration

■ permit (ARP access-list configuration)

Command History	Release	Modification
	12.2(25)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
	arp access-list	Defines an ARP ACL.
	deny (ARP access-list configuration)	Denies an ARP packet based on matches against the DHCP bindings.
	ip arp inspection filter vlan	Permits ARP requests and responses from a host configured with a static IP address.
	show arp access-list	Displays detailed information about ARP access lists.

police

Use the **police** policy-map class configuration command to define a single-rate traffic policer for a class of traffic. 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 an existing policer.

police *rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}]

no police *rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}]

Syntax Description		
<i>rate-bps</i>		Specify the average traffic rate in bps. The range is 8000 to 1000000000.
<i>burst-byte</i>		Specify the normal burst size in bytes. The range is 8000 to 1000000.
exceed-action drop	(Optional)	When the specified rate is exceeded, specify that the switch drop the packet.
exceed-action policed-dscp-transmit	(Optional)	When the specified rate is exceeded, specify that the switch change the Differentiated Services Code Point (DSCP) of the packet to that specified in the policed-DSCP map and then send the packet.
Note This exceed-action policed-dscp-transmit keywords are not supported in ingress and egress hierarchical policies on enhanced-services (ES) ports.		

Defaults No policers are defined.

Command Modes Policy-map class configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines On a standard port and on the input of an ES port, the port ASIC device that controls the ports supports 256 policers on the switch (255 user-configurable policers plus 1 policer reserved for system internal use). The maximum number of policers that can be configured per port is 63. Policers are allocated on demand by the software and are constrained by the hardware and ASIC boundaries. You cannot reserve policers per port. There is no guarantee that a port will be assigned to any policer. These limitations do not apply to policers configured in a hierarchical policy attached to an ES port.

In Cisco IOS Release 12.2(25)EY or later, when configuring hierarchical dual-level policy maps, you can only use the **police** policy-map command in a secondary interface-level policy map.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Policing uses a token-bucket algorithm. You configure the bucket depth (the maximum burst that is tolerated before the bucket overflows) by using the *burst-byte* option of the **police** policy-map class configuration command or the **mls qos aggregate-policer** global configuration command. You configure

how quickly (the average rate) the tokens are removed from the bucket by using the *rate-bps* option of the **police** policy-map class configuration command or the **mls qos aggregate-policer** global configuration command. For more information, see the software configuration guide for this release.

Examples

This example shows how to configure a policer that drops packets if traffic exceeds 1 Mbps average rate with a burst size of 20 KB. The DSCP values of inbound packets are trusted, and there is no packet modification.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set ip dscp 45
Switch(config-pmap-c)# police 1000000 20000 exceed-action drop
Switch(config-pmap-c)# exit
```

This example shows how to configure a policer, which marks down the DSCP values with the values defined in policed-DSCP map and sends the packet:

```
Switch(config)# policy-map policy2
Switch(config-pmap)# class class2
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
```

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

Related Commands

Command	Description
class	Specifies the name of the class whose traffic policy you want to create or change.
mls qos map policed-dscp	Defines the policed-DSCP map.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map	Displays quality of service (QoS) policy maps.

police aggregate

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*

Syntax Description	<i>aggregate-policer-name</i> Name of the aggregate policer.

Defaults	No aggregate policers are defined.

Command Modes	Policy-map class configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	On standard ports and enhanced-services (ES) ports, the port ASIC device that controls the ports supports 256 policers on the switch (255 user-configurable policers plus 1 policer reserved for system internal use). The maximum number of policers that can be configured per port is 63. Policers are allocated on demand by the software and are constrained by the hardware and ASIC boundaries. You cannot reserve policers per port. There is no guarantee that a port will be assigned to any policer. These limitations do not apply to policers configured in a hierarchical policy attached to an ES port.

You set aggregate policer parameters by using the **mls qos aggregate-policer** global configuration command. You apply an aggregate policer to multiple classes in the same policy map; you cannot use an aggregate policer across different policy maps.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

In Cisco IOS Release 12.2(25)EY or later, you can configure aggregate policers only in nonhierarchical single-level policy maps.

Examples	This example shows how to define the aggregate policer parameters and to apply the policer to multiple classes in a policy map:

```
Switch(config)# mls qos aggregate-policer agg_policer1 10000 1000000 exceed-action drop
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# set ip dscp 10
```

police aggregate

```
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate agg_policer2
Switch(config-pmap-c)# exit
```

You can verify your settings by entering the **show mls qos aggregate-policer** privileged EXEC command.

Related Commands

Command	Description
mls qos aggregate-policer	Defines policer parameters, which can be shared by multiple classes within the same policy map.
show mls qos aggregate-policer	Displays the quality of service (QoS) aggregate policer configuration.

police cir

Use the **police cir** policy-map class configuration command to configure a hierarchical traffic policer that uses two rates, the committed information rate (CIR) and the peak information rate (PIR) on an enhanced-services (ES) port. Use the **no** form of this command to remove the two-rate policer.

```
police cir cir [bc conform-burst] pir pir [be peak-burst] [conform-action action [exceed-action action [violate-action action]]]
```

```
no police cir cir [bc conform-burst] pir pir [be peak-burst] [conform-action action [exceed-action action [violate-action action]]]
```

Syntax Description	
cir <i>cir</i>	CIR at which the first token bucket is updated. The range is 64000 to 990000000 bps.
bc <i>conform-burst</i>	(Optional) Conform burst size used by the first token bucket for policing. The range is 1536 to 16776960 bytes.
pir <i>pir</i>	PIR at which the second token bucket for policing is updated. The range is 64000 to 990000000 bps.
be <i>peak-burst</i>	(Optional) Peak burst size used by the second token bucket. The range is 1536 to 16776960 bytes.
conform-action	(Optional) Action to perform on packets that conform to the CIR and PIR.
exceed-action	(Optional) Action to perform on packets that conform to the PIR but not the CIR.
violate-action	(Optional) Action to perform on packets that exceed the PIR.
<i>action</i>	(Optional) Action to perform on packets. The keywords have these meanings: • drop—drop the packet. • set-cos-transmit <i>new-cos</i>—set the class of service (CoS) value to a new value and send the packet. The range is 0 to 7. • set-dscp-transmit <i>new-dscp</i>—set the IP Differentiated Services Code Point (DSCP) value to a new value and send the packet. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value. • set-mpls-exp-transmit <i>new-exp</i>—set the multiprotocol label switching (MPLS) experimental bits and send the packet. The range is 0 to 7. • set-prec-transmit <i>new-prec</i>—set the IP precedence value to a new value and send the packet. The range is 0 to 7. • transmit—send the packet without altering it.

Defaults

No policers are defined. The default conform burst size (bc) and peak burst size (be) is 8192 bytes.

If no action is specified, the default **conform-action** is transmit, the default **exceed-action** is drop, and the default **violate-action** is drop.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.
12.2(25)EY	Hierarchical service policies can be attached to inbound traffic received on an ES port.

Usage Guidelines

Use the **police cir** policy-map class configuration command only in a hierarchical policy map attached to an ES port. This command is valid in policy maps at any level of the hierarchy.

You enforce traffic policing on a port at the edge of a network by limiting the transmission rate of a traffic class and by marking actions for each packet (conform, exceed, and violate). Within these categories, you decide packet treatments. In the most common configurations, you can configure packets that conform to be sent, packets that exceed to be sent with a decreased priority, and packets that violate to be dropped. You can decrease the priority of the CoS, the DSCP, the IP precedence, or the MPLS experimental bits.

The two-rate policer manages the maximum rate of traffic through a token-bucket algorithm, which uses the configured values to control the maximum rate of traffic allowed on a port at a given moment in time. The token-bucket algorithm is affected by all traffic leaving the port and manages network bandwidth when several large packets are sent in the same traffic stream.

A token bucket is provided for the CIR and the PIR. You configure the CIR and PIR rates in bps, controlling how fast the bucket fills (is updated) with tokens. The conform burst size and the peak burst size represent the depth of the CIR and PIR buckets in bytes. This depth limits the number of tokens that the bucket can accumulate. If the bucket fills to capacity, newly arriving tokens are discarded.

Each token is permission for the source to send a certain number of bits into the network. To send a packet, the number of tokens equal to the packet size must be drained from the bucket. If there are enough tokens in the bucket, the packet conforms and can pass to the next stage. Otherwise, the exceed action associated with the bucket is applied to the packet. The packet might be dropped, or its priority value might be marked down.

In this token-bucket example, if the CIR rate is 2 kbps, 2000 tokens are added to the bucket every second (for this example, consider each token to represent a single bit of information). If a 1500-byte packet arrives, 12000 tokens (1500 bytes x 8 bits per byte) must be in the bucket for the packet to pass to the next state without triggering the exceed action. If enough tokens are in the bucket, they are drained, and the packet conforms and passes to the next stage. If there are less than 12000 tokens in the bucket, the exceed action is applied to the packet. The deeper the bucket, the more data can burst through at a rate greater than the rate at which the bucket is filling. For example, if the CIR bucket holds 6000 tokens, 750 bytes of traffic can instantaneously burst without draining the bucket (and without triggering an exceed action), even though the instantaneous burst is at a greater rate than the CIR rate of 2000 bps.

If the burst sizes approach the system maximum transmission unit (MTU), the policer strictly enforces the CIR and PIR. Normal traffic jitter can cause some percentage of inbound traffic to be flagged as nonconforming even if the average inbound rate appears to conform. If the burst size is very large, on the other hand, large traffic bursts at nonconforming data rates can be passed through the policer and flagged as conforming. Setting the burst sizes too low can result in less traffic than expected, and setting them too high can result in more traffic than expected.

For packet marking actions, if the CIR is 100 kbps, the PIR is 200 kbps, and a data stream with a rate of 250 kbps arrives at the two-rate policer, this is the packet marking:

- 100 kbps is marked as conforming to the rate.
- 100 kbps is marked as exceeding the rate.
- 50 kbps is marked as violating the rate.

If you set the CIR equal to the PIR, a traffic rate that is less than the CIR or that meets the CIR is in the conform range. A traffic that exceeds the CIR rate is in the violate range.

If you set the PIR greater than the CIR, a traffic rate less than the CIR is in the conform range. A traffic rate that exceeds the CIR but is less than or equal to the PIR is in the exceed range. A traffic rate that exceeds the PIR is in the violate range.

If you apply a single-rate traffic policer to an ES port by using the **police rate-bps burst-byte [exceed-action {drop | policed-dscp-transmit}]** policy-map class configuration command, the software automatically sets the CIR and the PIR to the same value.

Examples

This example shows how to configure a two-rate traffic policer on a class to limit traffic to an average committed rate of 500 kbps and a peak rate of 1 Mbps:

```
Switch(config)# class-map c1
Switch(config-cmap)# match ip precedence 4
Switch(config-cmap)# exit
Switch(config)# policy-map policy1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config-pmap-c)# interface gigabitethernet1/1/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# end
```

Traffic marked as conforming to the average committed rate (500 kbps) is sent as is. Traffic marked as exceeding 500 kbps, but not exceeding 1 Mbps, is marked with IP precedence 2 and then sent. All traffic marked as exceeding 1 Mbps is dropped. The burst parameters are set to 10000 bytes.

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

Related Commands

Command	Description
class	Specifies the name of the class whose traffic policy you want to create or change.
police cir percent	Configures a two-rate traffic policer for a class of traffic based on a percentage of the available bandwidth on an ES port.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map	Displays quality of service (QoS) policy maps.
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.

police cir percent

Use the **police cir percent** policy-map class configuration command to configure a traffic policer that uses two rates, the committed information rate (CIR) and the peak information rate (PIR), and is based on a percentage of bandwidth available on an enhanced-services (ES) port. Use the **no** form of this command to remove the traffic policer configuration.

```
police cir percent percent [bc conform-burst ms] | pir percent percent [be peak-burst ms]
[conform-action action [exceed-action action [violate-action action]]]
```

```
no police cir percent percent [bc conform-burst ms] | pir percent percent [be peak-burst ms]
[conform-action action [exceed-action action [violate-action action]]]
```

Syntax Description

<i>percent</i>	Percentage of the available bandwidth assigned to the parent class. This value is used for calculating the CIR (the rate at which the first token bucket for policing is updated). The range is from 1 to 99.
bc conform-burst ms	(Optional) Conform burst size used by the first token bucket for policing. The range is 1 to 128 ms.
pir percent percent	Percentage of the available bandwidth assigned to the parent class. This value is used for calculating the PIR (the rate at which the second token bucket for policing is updated). The range is 1 to 99.
be peak-burst ms	(Optional) Peak burst size used by the second token bucket. The range is 1 to 128 ms.
conform-action	(Optional) Action to perform on packets that conform to the CIR and PIR.
exceed-action	(Optional) Action to perform on packets that conform to the PIR but not the CIR.
violate-action	(Optional) Action to perform on packets that exceed the PIR.
<i>action</i>	(Optional) Action to perform on packets. The keywords have these meanings: • drop—drop the packet. • set-cos-transmit new-cos—set the class of service (CoS) value to a new value and send the packet. The range is 0 to 7. • set-dscp-transmit new-dscp—set the IP Differentiated Services Code Point (DSCP) value to a new value and send the packet. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value. • set-mpls-exp-transmit new-exp—set the multiprotocol label switching (MPLS) experimental bits and send the packet. The range is 0 to 7. • set-prec-transmit new-prec—set the IP precedence value to a new value and send the packet. The range is 0 to 7. • transmit—send the packet without altering it.

Defaults

No policers are defined.

If no action is specified, the default **conform-action** is transmit, the default **exceed-action** is drop, and the default **violate-action** is drop.

Command Modes Policy-map class configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.
	12.2(25)EY	Hierarchical service policies can be attached to inbound traffic received on an ES port.

Usage Guidelines

Use the **police cir percent** policy-map class configuration command only in a hierarchical policy map attached to an ES port. This command is valid in policy maps at any level of the hierarchy.

You can create a three-level (nested) hierarchy: a primary (or *parent*) level in the physical-level policy map, a secondary (or *child*) level in the VLAN-level policy map, and a third child level in the class-level policy map. Note that the VLAN-level configuration is the parent of the class-level configuration.

The switch calculates the CIR and PIR based on a percentage of the maximum amount of bandwidth assigned to the parent class. The maximum bandwidth is controlled by the **shape** policy-map class configuration command if it is configured. Otherwise, the maximum bandwidth is the physical port bandwidth (1 Gbps).

When you specify the CIR and PIR rates as a percentage in a class-level child policy, the switch uses the maximum bandwidth amount that is specified in the next higher-level policy (in this case, the parent's maximum bandwidth at the VLAN level) to calculate the rates in bps. If the VLAN-level policy does not specify a maximum bandwidth, the switch uses the maximum bandwidth of the parent's parent (the physical-level policy). If the physical-level policy does not specify a maximum bandwidth, the switch uses the bandwidth of the physical port to calculate the rates in bps. The **police cir percent** command always refers to the next higher level for the maximum bandwidth reference point. For more information, see the "Examples" section.

The calculated CIR and PIR bps rates must be in the range of 8000 and 2000000000 bps. If the rates are outside this range, the switch does not attach the policy map to the port. If the port bandwidth changes (for example, more is added), the switch recalculates the bps values of the CIR and the PIR based on the revised amount of bandwidth. If the CIR and PIR percentages are changed after the policy map is attached to the port, the switch recalculates the bps values of the CIR and PIR.

Setting the burst sizes too low can result in more traffic than expected, and setting them too high can result in less traffic than expected. Both of these conditions can violate the policer checks.

If you want the policer to be calculated as a percentage, specify the conform burst size and the peak burst size in ms.

If you configure the **conform-action**, **exceed-action**, **violate-action** in a two-rate ingress policer and set the CoS, DSCP, or IP precedence values of the packet by using the **set-cos-transmit new-cos**, **set-dscp-transmit new-dscp**, or the **set-prec-transmit new-prec** options, the switch automatically applies the port trust state to all traffic received on the ES port, including traffic that does not match the traffic class with the two-rate policer.

You cannot combine Layer 2 (**set-cos-transmit new-cos**) and Layer 3 (**set-dscp-transmit new-dscp**, or the **set-prec-transmit new-prec**) actions in a two-rate ingress policer because the port can trust only one value in the inbound packet (CoS, DSCP, or IP precedence). For example, you cannot configure the **police cir percent 10 conform-action set-cos-transmit 3 exceed-action set dscp-transmit af22** command. The **conform-action** sets the CoS value to 3 while the **exceed-action** sets the DSCP value to af22.

Examples

This example shows how to configure traffic policing by using a CIR and a PIR based on a percentage of bandwidth. In this example, a CIR of 20 percent and a PIR of 40 percent are specified. The optional **bc** and **be** values (300 ms and 400 ms, respectively) are specified.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police cir percent 20 bc 300 ms pir percent 40 be 400 ms
conform-action transmit exceed-action set-prec-transmit 2 violate-action drop
Switch(config-pmap-c)# service-policy child-policy1
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# service-policy input policy1
```

This example shows how to create two hierarchical policies, one called *child_policy* and one called *parent_policy*. In the *child_policy* policy-map, the **police cir percent** command is configured in the class called *normal_type*. In this class, the percentage specified by the **police cir percent** command is 30 percent. The command uses 512 kbps, the peak rate (specified in the *parent_policy* through the **shape average 512000** command), as the bandwidth reference point for the *class parent* in the *parent_policy*. The **police cir percent** command uses 512 kbps as the basis for calculating the CIR rate (512 kbps * 30 percent).

```
Switch(config)# policy-map child_policy
Switch(config-pmap)# class normal_type
Switch(config-pmap-c)# police cir percent 30
Switch(config-pmap-c)# exit
Switch(config)# policy-map parent_policy
Switch(config-pmap)# class parent
Switch(config-pmap-c)# shape average 512000
Switch(config-pmap-c)# service-policy child_policy
Switch(config-pmap-c)# exit
```

This example shows how to create two hierarchical policies, one called *child_policy* and one called *parent_policy*. In the *child_policy* policy map, the **police cir percent** command is configured in the class called *normal_type*. In this class, the percentage specified by the **police cir percent** command is 30 percent. In the *parent_policy*, a peak rate is not specified. The **bandwidth** policy-map class configuration command is used, but this command does not represent the maximum rate of bandwidth available. Therefore, the **police cir percent** command uses the next higher level (Gigabit Ethernet port) as the bandwidth reference point. Assuming the bandwidth of the port is 1 Mbps, the **police cir percent** command uses 1 Mbps as the basis for calculating the CIR rate (1000000 * 30 percent).

```
Switch(config)# policy-map child_policy
Switch(config-pmap)# class normal_type
Switch(config-pmap-c)# police cir percent 30
Switch(config-pmap-c)# exit
Switch(config)# policy-map parent_policy
Switch(config-pmap)# class parent
Switch(config-pmap-c)# bandwidth 512
Switch(config-pmap-c)# service-policy child_policy
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# service-policy output parent_policy
Switch(config-if)# exit
```

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

Related Commands	Command	Description
	class	Specifies the name of the class whose traffic policy you want to create or change.
	police cir	Configures a two-rate traffic policer for a class of traffic.
	policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
	show policy-map	Displays quality of service (QoS) policy maps.
	show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.

policy-map

Use the **policy-map** global configuration command to create or modify a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode. Use the **no** form of this command to delete an existing policy map and to return to global configuration mode.

policy-map *policy-map-name*

no policy-map *policy-map-name*

Syntax Description

<i>policy-map-name</i>	Name of the policy map.

Defaults

No policy maps are defined.

The default behavior is to set the Differentiated Services Code Point (DSCP) to 0 if the packet is an IP packet and to set the class of service (CoS) to 0 if the packet is tagged. No policing is performed.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.
12.2(25)EY	Support for policy maps on switch virtual interfaces (SVIs) was added.

Usage Guidelines

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. After you enter the **policy-map** command, the switch enters policy-map configuration mode. You can configure or modify the class policies for that policy map and decide how to treat the classified traffic.

These configuration commands are available in policy-map configuration mode:

- **class**: defines the classification match criteria for the specified class map. For more information, see the “[class](#)” section on page 2-35.
- **description**: describes the policy map (up to 200 characters).
- **exit**: exits policy-map configuration mode and returns you to global configuration mode.
- **no**: removes a previously defined policy map.
- **rename**: renames the current policy map.

To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

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.

Only one policy map per port is supported. With standard QoS, you can attach one ingress nonhierarchical single-level service policy per standard physical port, per SVI, or per enhanced-services (ES) port. You can also apply one ingress hierarchical dual-level hierarchical service policy per SVI. With hierarchical QoS on ES ports, you can attach one ingress hierarchical service policy and one egress hierarchical service policy per ES port. If an ingress hierarchical service policy is attached to a ES port, the service policy must have at least two levels.

You can apply the same policy map to multiple ports. When you attempt to attach a policy map to a port, the attempt is denied if the available bandwidth on the port cannot accommodate the total bandwidth requested by class policies comprising the policy map.

Whenever you modify a class policy in an attached policy map, class-based weighted fair queueing (CBWFQ) is notified, and the new classes are installed as part of the policy map in the CBWFQ system.

In software releases earlier than Cisco IOS Release 12.2(25)EY, you can apply a policy map and configure policing only on physical ports. You can configure the trust state, set a new DSCP or IP precedence value in the packet, or define an individual or aggregate policer.

In Cisco IOS Release 12.2(25)EY or later, you can apply a nonhierarchical single-level policy map to ingress physical ports, SVIs, or ES ports. A single-level policy map is the same as a standard port-based policy map in software releases earlier than Cisco IOS Release 12.2(25)EY. However, a hierarchical dual-level policy map can be applied only to SVIs, and a hierarchical policy map can be applied only to ES ports.

A dual-level policy map has two levels. The first level, the VLAN level, specifies the actions to be taken against a traffic flow on an SVI. The second level, the interface level, specifies the actions to be taken against the traffic on the physical ports that belong to the SVI and are specified in the interface-level policy map. In a primary VLAN-level policy map, you can only configure the trust state or set a new DSCP or IP precedence value in the packet. In a secondary interface-level policy map, you can only configure individual policers on physical ports that belong to the SVI.

After the dual-level policy map is attached to an SVI, an interface-level policy map cannot be modified or removed from the dual-level policy map. A new interface-level policy map also cannot be added to the dual-level policy map. You also cannot add or remove a class map specified in the dual-level policy map. If you want these changes to occur, the dual-level policy map must first be removed from the SVI.

For more information about nonhierarchical single-level policy maps and hierarchical dual-level policy maps, see the “Ingress Policing and Marking” section in the “Configuring QoS” chapter of the software configuration guide for this release.

Examples

This example shows how to create a policy map called *policy1*. When attached to the ingress direction, it matches all the inbound traffic defined in *class1*, sets the IP DSCP to 10, and polices the traffic at an average rate of 1 Mbps and bursts at 20 KB. Traffic exceeding the profile is marked down to a DSCP value obtained from the policed-DSCP map and then sent.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set ip dscp 10
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
```

This example shows how to configure multiple classes in a policy map called *polycymap2*:

```
Switch(config)# policy-map polycymap2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set ip dscp 10
Switch(config-pmap-c)# police 100000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
```

```
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 100000 20000 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# set ip dscp 0
Switch(config-pmap-c)# exit
```

This example shows how to create a dual-level policy map and attach it to an SVI:

```
Switch(config)# class-map cm-non-int
Switch(config-cmap)# match access-group 101
Switch(config-cmap)# exit
Switch(config)# class-map cm-non-int-2
Switch(config-cmap)# match access-group 102
Switch(config-cmap)# exit
Switch(config)# class-map cm-test-int
Switch(config-cmap)# match input-interface gigabitethernet1/0/1 - gigabitethernet1/0/2
Switch(config-cmap)# exit
Switch(config)# policy-map pm-test-int
Switch(config-pmap)# class cm-test-int
Switch(config-pmap-c)# police 18000000 8000 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map pm-test-pm-2
Switch(config-pmap)# class cm-non-int
Switch(config-pmap-c)# set dscp 7
Switch(config-pmap-c)# service-policy pm-test-int
Switch(config-pmap)# class cm-non-int-2
Switch(config-pmap-c)# set dscp 15
Switch(config-pmap-c)# service-policy pm-test-int
Switch(config-pmap-c)# end
Switch(config-cmap)# exit
Switch(config)# interface vlan 10
Switch(config-if)# service-policy input pm-test-pm-2
```

This example shows how to delete *polycymap2*:

```
Switch(config)# no policy-map polycymap2
```

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

Related Commands

Command	Description
class	Specifies the name of the class whose traffic policy you want to create or change.
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
service-policy (interface configuration)	Applies a policy map to a port.
show policy-map	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	
dst-ip	Load distribution is based on the destination host IP address.
dst-mac	Load distribution is based on the destination host MAC address. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel.
src-dst-ip	Load distribution is based on the source and destination host IP address.
src-dst-mac	Load distribution is based on the source and destination host MAC address.
src-ip	Load distribution is based on the source host IP address.
src-mac	Load distribution is based on the source MAC address. Packets from different hosts use different ports in the channel, but packets from the same host use the same port.

Defaults The default is **src-mac**.

Command Modes Global configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines For information about when to use these forwarding methods, see the “Configuring EtherChannels” chapter in the software guide for this release.

Examples This example shows how to set the load-distribution method to **dst-mac**:

```
Switch(config)# port-channel load-balance dst-mac
```

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

Related Commands	Command	Description
	interface port-channel	Accesses or creates the port channel.

Command	Description
show etherchannel	Displays EtherChannel information for a channel.
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.

priority

Use the **priority** policy-map class configuration command to enable the strict priority queue (low-latency queueing [LLQ]) and to give priority to a class of traffic belonging to a hierarchical policy map attached to an enhanced-services (ES) port. Use the **no** form of this command to return to the default setting.

priority

no priority

Syntax Description This command has no arguments or keywords.

Defaults The strict priority queue is disabled.

Command Modes Policy-map class configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.
	12.2(25)EY	Hierarchical service policies can be attached to inbound traffic received on an ES port.

Usage Guidelines Use the **priority** command only in a hierarchical policy map attached to an ES port. You can use this command only in class-level classes.

This command configures LLQ and provides strict-priority queueing for class-based weighted fair queueing (CBWFQ). Strict-priority queueing enables delay-sensitive data, such as voice, to be sent before packets in other queues are sent. The priority queue is serviced first until it is empty.

You cannot use the **bandwidth**, **queue-limit**, **random-detect**, and the **shape** policy-map class configuration commands with the **priority** policy-map class configuration command in the same class within the same policy map. However, you can use these commands in the same policy map.

Within a policy map, you can give priority status to only one class.

When you attach the policy map containing class policy configurations to the port to stipulate the service policy for that port, the available bandwidth is determined.

To avoid a loss of priority traffic on an ES port when the switch is congested, you can configure both the strict-priority queueing and egress priority queueing features. Note that when you map certain traffic classes to the egress priority queue, they are not automatically placed into the strict-priority queue. You must configure both the **priority** policy-map class configuration and the **priority-queue out** interface configuration commands. For more information, see the [“priority-queue” section on page 2-327](#).

Examples

This example shows how to enable the LLQ for the policy map called *policy1*:

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class voice
Switch(config-pmap-c)# priority
```

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

Related Commands

Command	Description
bandwidth	Specifies or modifies the minimum bandwidth provided to a class belonging to a policy map attached to an ES port.
class	Specifies the name of the class whose traffic policy you want to create or change.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
priority-queue	Enables the egress priority queue on a port.
queue-limit	Configures the maximum threshold for tail drop in a policy map attached to an ES port.
random-detect	Configures Weighted Random Early Detection (WRED) in a policy map attached to an ES port.
service-policy (policy-map class)	Creates a service policy as a quality of service (QoS) policy within a policy map.
shape	Enables traffic shaping in a policy map attached to an ES port.
show policy-map	Displays QoS policy maps.

priority-queue

Use the **priority-queue** interface configuration command to enable the egress priority queue on a port. Use the **no** form of this command to return to the default setting.

priority-queue out

no priority-queue out

Syntax Description

out	Enable the egress priority queue.

Defaults

The egress priority queue is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)AX2	This command was introduced.

Usage Guidelines

When you configure the **priority-queue out** command, the shaped round robin (SRR) weight ratios are affected because there is one fewer queue participating in SRR. This means that *weight1* in the **srr-queue bandwidth shape** or the **srr-queue bandwidth share** interface configuration command is ignored (not used in the ratio calculation). Before servicing the other queues, SRR services the priority queue until it is empty.

Follow these guidelines when the priority queue is enabled; otherwise, the egress queues are serviced based on their SRR weights:

- If the egress priority queue is enabled, it overrides the SRR shaped and shared weights for queue 1.
- If the egress priority queue is disabled and the SRR shaped and shared weights are configured, the shaped mode overrides the shared mode for queue 1, and SRR services this queue in shaped mode.
- If the egress priority queue is disabled and the SRR shaped weights are not configured, SRR services the queue in shared mode.

To avoid a loss of priority traffic on an enhanced-services (ES) port when the switch is congested, you can configure both the egress priority queueing and the strict-priority queueing (low-latency queueing [LLQ]) features. Note that when you map certain traffic classes to the egress priority queue, they are not automatically placed into the strict-priority queue. You must configure both the **priority-queue out** interface configuration and the **priority** policy-map class configuration commands. For more information, see the [“priority” section on page 2-325](#).

Examples

This example shows how to enable the egress priority queue when the SRR weights are configured. The egress expedite queue overrides the configured SRR weights.

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# srr-queue bandwidth shape 25 0 0 0
```

```
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# priority-queue out
```

This example shows how to disable the egress priority queue after the SRR shaped and shared weights are configured. The shaped mode overrides the shared mode.

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# srr-queue bandwidth shape 25 0 0 0
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# no priority-queue out
```

You can verify your settings by entering the **show mls qos interface *interface-id* queueing** or the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show mls qos interface queueing	Displays the queueing strategy (SRR, priority queueing), the weights corresponding to the queues, and the CoS-to-egress-queue map.
srr-queue bandwidth shape	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.
srr-queue bandwidth share	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

private-vlan

Use the **private-vlan** VLAN configuration command on the switch stack or on a standalone switch 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}

This command is available only if the switch stack master is running the enhanced multilayer image (EMI). We strongly recommend that the stack members also run the EMI when private VLANs are configured.

Syntax Description

association	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.
add	Associate a secondary VLAN to a primary VLAN.
remove	Clear the association between a secondary VLAN and a primary VLAN.
community	Designate the VLAN as a community VLAN.
isolated	Designate the VLAN as a community VLAN.
primary	Designate the VLAN as a community VLAN.



Note

The switch must be in VTP transparent mode when you configure private VLANs.

Defaults

The default is to have no private VLANs configured.

Command Modes

VLAN configuration

Command History

Release	Modification
12.2(25)EY	This command was introduced.

Usage Guidelines

Before configuring private VLANs, you must disable VTP (VTP mode transparent). After you configure a private VLAN, you should not change the VTP mode to client or server.

VTP does not propagate private-VLAN configuration. 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 in 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.

An **isolated** VLAN is used by isolated ports to communicate with promiscuous ports. It does not carry traffic to other community ports or 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.

Do not configure a private VLAN as a Remote Switched Port Analyzer (RSPAN) VLAN.

Do not configure a private VLAN as a voice VLAN.

Do not configure fallback bridging on switches with private VLANs.

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 mode 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, and VLANs 502 and 503 as community VLANs, and to associate them in a private VLAN:

```
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)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 503
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
	show interfaces status	Displays the status of interfaces, including the VLANs to which they belong.
	show vlan private-vlan	Displays the private VLANs and VLAN associations configured on the switch.
	switchport mode private-vlan	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) on the switch stack or on a standalone switch to create a mapping between a private-VLAN primary and secondary VLANs so that both VLANs share the same primary VLAN SVI. Use the **no** form of this command to remove private-VLAN mappings from the SVI.

private-vlan mapping {[add | remove] *secondary-vlan-list*}

no private-vlan mapping

This command is available only if the switch stack master is running the enhanced multilayer image (EMI). We strongly recommend that the stack members also run the EMI when private VLANs are configured.

Syntax Description	<i>secondary-vlan-list</i>	Specify one or more secondary VLANs to be mapped to the primary VLAN SVI.
	add	(Optional) Map the secondary VLAN to the primary VLAN SVI.
	remove	(Optional) Remove the mapping between the secondary VLAN and the primary VLAN SVI.



Note

The switch must be in VTP transparent mode when you configure private VLANs.

Defaults The default is to have no private VLAN SVI mapping configured.

Command Modes Interface configuration

Command History	Release	Modification
	12.2(25)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 SVI of the primary VLAN.

A secondary VLAN can be mapped to only one primary SVI. 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
show interfaces private-vlan mapping	Display private-VLAN mapping information for the VLAN SVIs.

queue-limit

Use the **queue-limit** policy-map class configuration command to configure the maximum threshold for tail drop in a hierarchical policy map attached to an enhanced-services (ES) port. Use the **no** form of this command to return to the default setting.

queue-limit *limit*

no queue-limit

Syntax Description	<i>limit</i> Queue maximum threshold on an ES port. The range is 1 to 32768 packets.

Defaults	The maximum threshold is 128 packets.

Command Modes	Policy-map class configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.
	12.2(25)EY	Hierarchical service policies can be attached to inbound traffic received on an ES port.

Usage Guidelines

Class-based weighted fair queueing (CBWFQ) creates a queue for every class for which a class map is defined. Packets satisfying the match criteria for a class accumulate in the queue reserved for the class until they are sent, which occurs when the queue is serviced by the fair queue process. When the maximum packet threshold you defined for the class is reached, any more packets destined for the class queue are dropped according to the tail drop or Weighted Random Early Detection (WRED) mechanism. With tail drop, packets are queued until the maximum threshold is exceeded, and then all the packets are dropped.

Use the **queue-limit** command only in a hierarchical policy map attached to an ES port. You can use this command only in class-level classes.

You must configure the **bandwidth** or the **shape** policy-map class configuration command before you configure either the **queue-limit** or the **random-detect** policy-map class configuration command in a class policy.

You can define a class policy to use either tail drop through the **queue-limit** policy-map class configuration command or to use WRED packet drop through the **random-detect** policy-map class configuration command. You cannot use the **queue-limit** and **random-detect** commands in the same class policy, but they can be used in two class policies in the same policy map.

You cannot use the **bandwidth**, **queue-limit**, **random-detect**, and the **shape** policy-map class configuration commands with the **priority** policy-map class configuration command in the same class within the same policy map. However, you can use these commands in the same policy map.

Examples

This example shows how to create a policy map called *policy11* for a class called *acl203*. In the policy for this class, the queue maximum threshold is set to 30000 packets:

```
Switch(config)# policy-map policy11
Switch(config-pmap)# class acl203
Switch(config-pmap-c)# bandwidth 2000
Switch(config-pmap-c)# queue-limit 30000
```

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

Related Commands

Command	Description
bandwidth	Specifies or modifies the minimum bandwidth provided to a class belonging to a policy map attached to an ES port.
class	Specifies the name of the class whose traffic policy you want to create or change.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
priority	Enables the strict-priority queue and gives priority to a class of traffic belonging to a policy map attached to an ES port.
random-detect	Configures WRED in a policy map attached to an ES port.
service-policy (policy-map class)	Creates a service policy as a quality of service (QoS) policy within a policy map.
show policy-map	Displays QoS policy maps.

queue-set

Use the **queue-set** interface configuration command to map a port to a queue-set. Use the **no** form of this command to return to the default setting.

queue-set *qset-id*

no queue-set *qset-id*

Syntax Description	<i>qset-id</i> ID of the queue-set. Each port belongs to a queue-set, which defines all the characteristics of the four egress queues per port. The range is 1 to 2.	
Defaults	The queue-set ID is 1.	
Command Modes	Interface configuration	
Command History	Release	Modification
	12.1(14)AX	This command was introduced.
Examples	This example shows how to map a port to queue-set 2: <pre>Switch(config)# interface fastethernet1/0/1 Switch(config-if)# queue-set 2</pre> You can verify your settings by entering the show mls qos interface [interface-id] buffers privileged EXEC command.	
Related Commands	Command	Description
	mls qos queue-set output buffers	Allocates buffers to a queue-set.
	mls qos queue-set output threshold	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
	show mls qos interface buffers	Displays buffer allocation information.

random-detect

Use the **random-detect** policy-map class configuration command to enable Weighted Random Early Detection (WRED) in a hierarchical policy map attached to an enhanced-services (ES) port. Use the **no** form of this command to return to the default settings.

random-detect [**dscp-based** | **precedence-based**]

no random detect [**dscp-based** | **precedence-based**]

Syntax Description

dscp-based	(Optional) Enable Differentiated Services Code Point (DSCP)-based WRED as a drop policy. WRED uses the DSCP value (that is, the first six bits of the IP type of service [ToS] byte) to calculate the drop probability.
precedence-based	(Optional) Enable IP precedence-based WRED as a drop policy. WRED uses the IP precedence value to calculate the drop probability.

Defaults

WRED is disabled.

If you do not enter either the **dscp-based** or the **precedence-based** keyword, WRED uses the IP precedence value (the default method) to calculate drop probability for the packet.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.
12.2(25)EY	Hierarchical service policies can be attached to inbound traffic received on an ES port.

Usage Guidelines

WRED is a congestion-avoidance mechanism that slows traffic by randomly dropping packets when congestion exists. WRED reduces the chances of tail drop by selectively dropping packets when the egress port begins to show signs of congestion. By dropping some packets early rather than waiting until the queue is full, WRED does not drop large numbers of packets at once.

Use the **random-detect** command only in a hierarchical policy map attached to an ES port. You can use this command only in class-level classes.

You must configure the **bandwidth** or the **shape** policy-map class configuration command before you configure either the **queue-limit** or the **random-detect** policy-map class configuration command in a class policy.

You can define a class policy to use either tail drop or WRED packet drop by using either the **queue-limit** policy-map class configuration command or the **random-detect** policy-map class configuration command, respectively. You cannot use the **queue-limit** and **random-detect** commands in the same class policy, but they can be used in two class policies in the same policy map.

You cannot use the **bandwidth**, **queue-limit**, **random-detect**, and the **shape** policy-map class configuration commands with the **priority** policy-map class configuration command in the same class within the same policy map. However, you can use these commands in the same policy map.

If you use the **dscp-based** keyword, WRED uses the DSCP value to calculate the drop probability. If you use the **precedence-based** keyword, WRED uses the IP precedence value to calculate the drop probability. The **dscp-based** and **precedence-based** keywords are mutually exclusive. If you do not specify either argument, WRED uses the IP precedence value to calculate the drop probability (the default method).

You must enter the **random-detect dscp-based** command before specifying the values with the **random-detect dscp dscp min-threshold max-threshold mark-prob-denominator** command. You must enter the **random-detect precedence-based** command before specifying the values with the **random-detect precedence ip-precedence min-threshold max-threshold mark-prob-denominator** 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 configure the policy map called *policy1* that contains a policy specification for the class called *class1*. During times of congestion, IP precedence-based WRED packet drop is used instead of tail drop.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# bandwidth 1000
Switch(config-pmap-c)# random-detect
```

This example shows how to enable DSCP-based WRED as a drop policy. It uses the DSCP value 8 for class *c1*. The minimum threshold for DSCP value 8 is 24, the maximum threshold is 40, and the mark-probability denominator is 512. The last command attaches the service policy to the port.

```
Switch(config)# class-map c1
Switch(config-cmap)# match ip dscp 8
Switch(config-cmap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# bandwidth 48
Switch(config-pmap-c)# random-detect dscp-based
Switch(config-pmap-c)# random-detect dscp 8 24 40 512
Switch(config-pmap-c)# exit
Switch(config-pmap)# end
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# service-policy output p1
```

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

Related Commands

Command	Description
bandwidth	Specifies or modifies the minimum bandwidth provided to a class belonging to a policy map attached to an ES port.
class	Specifies the name of the class whose traffic policy you want to create or change.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.

Command	Description
priority	Enables the strict-priority queue and gives priority to a class of traffic belonging to a policy map attached to an ES port.
queue-limit	Configures the maximum threshold for tail drop in a policy map attached to an ES port.
random-detect dscp	Configures DSCP-based WRED settings in a policy map attached to an ES port.
random-detect exponential-weighting-constant	Configures WRED exponential weight factor for the average queue-size calculation for the queue in a policy map attached to an ES port.
random-detect precedence	Configures IP precedence-based WRED settings in a policy map attached to an ES port.
service-policy (policy-map class)	Creates a service policy as a quality of service (QoS) policy within a policy map.
shape	Enables traffic shaping in a policy map attached to an ES port.
show policy-map	Displays QoS policy maps.

random-detect dscp

Use the **random-detect dscp** policy-map class configuration command to configure Differentiated Services Code Point (DSCP)-based Weighted Random Early Detection (WRED) settings in a hierarchical policy map attached to an enhanced-services (ES) port. Use the **no** form of this command to return to the default settings.

random-detect dscp *dscp min-threshold max-threshold mark-prob-denominator*

no random detect dscp *dscp*

Syntax Description

<i>dscp min-threshold max-threshold mark-prob-denominator</i>	Specify WRED settings, such as packet-threshold and mark-probability values, for a DSCP value. Specify these options: <i>dscp</i>—DSCP value. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value. For more information, see the “Usage Guidelines” section. <i>min-threshold</i>—the minimum threshold in packets. The range is 1 to 32768. When the average queue size reaches the minimum threshold, WRED randomly drops some packets with the specified DSCP value. <i>max-threshold</i>—the maximum threshold in packets. The range is 1 to 32768. When the average queue size exceeds the maximum threshold, WRED drops all packets with the specified DSCP value. <i>mark-prob-denominator</i>—the denominator for the fraction of packets dropped when the average queue size is at the maximum threshold. The range is 1 to 65535. For example, if the denominator is 512, one out of every 512 packets is dropped when the queue is at the maximum threshold. The packet-drop probability is based on the minimum threshold, the maximum threshold, and the mark-probability denominator. The default is 10; 1 out of every 10 packets is dropped at the maximum threshold.

Defaults

If WRED is using the DSCP value to calculate the drop probability of a packet, all entries of the DSCP table are initialized with the default settings listed in [Table 2-15 on page 2-342](#). The *min-threshold* default is 64 packets, and the *max-threshold* default is 128 packets.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.
12.2(25)EY	Hierarchical service policies can be attached to inbound traffic received on an ES port.

Usage Guidelines

WRED is a congestion-avoidance mechanism that slows traffic by randomly dropping packets when congestion exists. WRED reduces the chances of tail drop by selectively dropping packets when the egress port begins to show signs of congestion. By dropping some packets early rather than waiting until the queue is full, WRED does not drop large numbers of packets at once.

Use the **random-detect dscp** command only in a hierarchical policy map attached to an ES port. You can use this command only in class-level classes.

You must configure the **bandwidth** or the **shape** policy-map class configuration command before you configure either the **queue-limit** or the **random-detect** policy-map class configuration command in a class policy.

You can define a class policy to use either tail drop or WRED packet drop by using either the **queue-limit** policy-map class configuration command or the **random-detect** policy-map class configuration command, respectively. You cannot use the **queue-limit** and **random-detect** commands in the same class policy, but they can be used in two class policies in the same policy map.

You cannot use the **bandwidth**, **queue-limit**, **random-detect**, and the **shape** policy-map class configuration commands with the **priority** policy-map class configuration command in the same class within the same policy map. However, you can use these commands in the same policy map.

You must enter the **random-detect dscp-based** command before specifying the values with the **random-detect dscp** *dscp min-threshold max-threshold mark-prob-denominator* command.

For the **dscp** *dscp* option, you can enter a mnemonic name for a commonly used value for assured forwarding (AF) code points, expedited forwarding (EF) code points, and class selector (CS) values. For example, you can enter the **dscp af11** command, which is the same as entering the **dscp 10** command. For a list of supported mnemonics, enter the **random-detect dscp ?** command to see the command-line help strings.

The AF code points enables a domain to offer four different levels (four different AF classes) of forwarding assurances for IP packets received from other (such as customer) domains. Each one of the four AF classes is allocated a certain amount of forwarding services (buffer space and bandwidth).

Within each AF class, IP packets are marked with one of three possible drop-precedence values (binary 2[010], 4[100], or 6[110]), which exist as the three lowest bits in the DSCP header. In congested network environments, the drop-precedence value of the packet determines the importance of the packet within the AF class. Packets with higher drop-precedence values are discarded before packets with lower drop-precedence values. The upper three bits of the IP DSCP value determine the AF class; the lower three bits determine the drop probability.

The EF code point is usually used to mark high-priority, time-sensitive data. The EF code point marking is equal to the highest IP precedence value; therefore, the EF code point is always equal to precedence value 7.

The CS values are equal to IP precedence values (for instance, cs1 is the same as IP precedence 1).

Set the *min-threshold* value high enough to maximize the link usages. If the minimum threshold is too low, packets might be dropped unnecessarily, and the transmission link is not fully used. The difference between the maximum threshold and the minimum threshold should be large enough to avoid global synchronization of TCP hosts. This can occur as multiple TCP hosts reduce their transmission rates. If the difference between the maximum and minimum thresholds is too small, many packets might be dropped at once, resulting in global synchronization.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Table 2-15 lists the default settings used by the **random-detect dscp** command for the DSCP value specified. The last row of the table (the row labeled *default*) shows the default settings used for any DSCP value not specifically shown in the table.

Table 2-15 *random-detect dscp Default Settings*

DSCP (Precedence)	Minimum Threshold	Maximum Threshold	Mark Probability
af11	32	40	1/10
af12	28	40	1/10
af13	24	40	1/10
af21	32	40	1/10
af22	28	40	1/10
af23	24	40	1/10
af31	32	40	1/10
af32	28	40	1/10
af33	24	40	1/10
af41	32	40	1/10
af42	28	40	1/10
af43	24	40	1/10
cs1	22	40	1/10
cs2	24	40	1/10
cs3	26	40	1/10
cs4	28	40	1/10
cs5	30	40	1/10
cs6	32	40	1/10
cs7	34	40	1/10
ef	36	40	1/10
rsvp	36	40	1/10
default	20	40	1/10

Examples

This example shows how to enable DSCP-based WRED as a drop policy. It uses the DSCP value 8 for class *c1*. The minimum threshold for DSCP value 8 is 24, the maximum threshold is 40, and the mark-probability denominator is 512. The last command attaches the service policy to the port.

```
Switch(config)# class-map c1
Switch(config-cmap)# match ip dscp 8
Switch(config-cmap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# bandwidth 48
Switch(config-pmap-c)# random-detect dscp-based
Switch(config-pmap-c)# random-detect dscp 8 24 40 512
Switch(config-pmap-c)# exit
Switch(config-pmap)# end
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# service-policy input p1
```

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

Related Commands	Command	Description
	bandwidth	Specifies or modifies the minimum bandwidth provided to a class belonging to a policy map attached to an ES port.
	class	Specifies the name of the class whose traffic policy you want to create or change.
	policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
	priority	Enables the strict-priority queue and gives priority to a class of traffic belonging to a policy map attached to an ES port.
	queue-limit	Configures the maximum threshold for tail drop in a policy map attached to an ES port.
	random-detect	Enables WRED in a policy map attached to an ES port.
	random-detect exponential-weighting-constant	Configures WRED exponential weight factor for the average queue-size calculation for the queue in a policy map attached to an ES port.
	service-policy (policy-map class)	Creates a service policy as a quality of service (QoS) policy within a policy map.
	shape	Enables traffic shaping in a policy map attached to an ES port.
	show policy-map	Displays QoS policy maps.

random-detect exponential-weighting-constant

Use the **random-detect exponential-weighting-constant** policy-map class configuration command to configure Weighted Random Early Detection (WRED) exponential weight factor for the average queue-size calculation for the queue in a hierarchical policy map attached to an enhanced-services (ES) port. Use the **no** form of this command to return to the default settings.

random-detect exponential-weighting-constant *weight*

no random detect exponential-weighting-constant

Syntax Description	<i>weight</i>	Configure the exponential weight factor for the average queue-size calculation for WRED. The range is 1 to 16.

Defaults	The default is 9.

Command Modes	Policy-map class configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.
	12.2(25)EY	Hierarchical service policies can be attached to inbound traffic received on an ES port.

Usage Guidelines	WRED is a congestion-avoidance mechanism that slows traffic by randomly dropping packets when congestion exists. WRED reduces the chances of tail drop by selectively dropping packets when the egress port begins to show signs of congestion. By dropping some packets early rather than waiting until the queue is full, WRED does not drop large numbers of packets at once.

Use the **random-detect exponential-weighting-constant** command only in a hierarchical policy map attached to an ES port. You can use this command only in class-level classes.

You must configure the **bandwidth** or the **shape** policy-map class configuration command before you configure either the **queue-limit** or the **random-detect** policy-map class configuration command in a class policy.

You can define a class policy to use either tail drop or WRED packet drop by using either the **queue-limit** policy-map class configuration command or the **random-detect** policy-map class configuration command, respectively. You cannot use the **queue-limit** and **random-detect** commands in the same class policy, but they can be used in two class policies in the same policy map.

You cannot use the **bandwidth**, **queue-limit**, **random-detect**, and the **shape** policy-map class configuration commands with the **priority** policy-map class configuration command in the same class within the same policy map. However, you can use these commands in the same policy map.

If you select a high value for the exponential weighting constant, it smooths the peaks and valleys in the queue size. The average queue size is unlikely to change very quickly, avoiding drastic swings in size. The WRED process will be slow to start dropping packets, but it might continue dropping packets for a time after the actual queue size has fallen below the minimum threshold. The slow-moving average accommodates temporary bursts in traffic.

If you select a low value for the exponential weighting constant, the average queue size closely tracks the current queue size. The resulting average might fluctuate with changes in the traffic levels. In this case, the WRED process responds quickly to long queues. When the queue falls below the minimum threshold, the process stops dropping packets. If the value is too low, WRED overreacts to temporary traffic bursts and drops traffic unnecessarily.

**Note**

The default WRED exponential weighting constant value is based on the best available data. We recommend that you do not change the parameters from their default values unless you have decided that your applications would benefit from the changed values.

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 policy for a class called *acl10* included in the policy map called *policy10*. Class *acl10* has these characteristics: a minimum of 2000 kbps of bandwidth are expected to be delivered to this class in the event of congestion, and a weight factor of 10 is used to calculate the average queue size. For congestion avoidance, WRED packet drop is used instead of tail drop. IP precedence is reset for levels 0 to 2.

```
Switch(config)# policy-map policy10
Switch(config-pmap)# class acl10
Switch(config-pmap-c)# bandwidth 2000
Switch(config-pmap-c)# random-detect
Switch(config-pmap-c)# random-detect exponential-weighting-constant 10
Switch(config-pmap-c)# random-detect precedence 0 32 256 100
Switch(config-pmap-c)# random-detect precedence 1 64 256 100
Switch(config-pmap-c)# random-detect precedence 2 96 256 100
```

This example shows how to configure the policy map *policy1* to contain policy specification for the class called *class1*. During times of congestion, WRED packet drop is used instead of tail drop. The weight factor used for the average queue-size calculation for the queue for *class1* is 12.

```
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 12
Switch(config-cmap)# exit
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# bandwidth 1000
Switch(config-pmap-c)# random-detect
Switch(config-pmap-c)# random-detect exponential-weighting-constant 12
```

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

Related Commands	Command	Description
	bandwidth	Specifies or modifies the minimum bandwidth provided to a class belonging to a policy map attached to an ES port.
	class	Specifies the name of the class whose traffic policy you want to create or change.
	policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
	priority	Enables the strict-priority queue and gives priority to a class of traffic belonging to a policy map attached to an ES port.
	queue-limit	Configures the maximum threshold for tail drop in a policy map attached to an ES port.
	random-detect	Enables WRED in a policy map attached to an ES port.
	random-detect dscp	Configures DSCP-based WRED settings in a policy map attached to an ES port.
	random-detect precedence	Configures IP precedence-based WRED settings in a policy map attached to an ES port.
	service-policy (policy-map class)	Creates a service policy as a quality of service (QoS) policy within a policy map.
	shape	Enables traffic shaping in a policy map attached to an ES port.
	show policy-map	Displays QoS policy maps.

random-detect precedence

Use the **random-detect precedence** policy-map class configuration command to configure IP precedence-based Weighted Random Early Detection (WRED) settings in a hierarchical policy map attached to an enhanced-services (ES) port. Use the **no** form of this command to return to the default settings.

random-detect precedence *ip-precedence min-threshold max-threshold mark-prob-denominator*

no random detect precedence *ip-precedence*

Syntax Description

<i>ip-precedence</i>	Specify WRED settings, such as packet threshold and mark probability values, for an IP precedence value. Specify these options:
<i>min-threshold</i>	
<i>max-threshold</i>	
<i>mark-prob-denominator</i>	
	• <i>ip-precedence</i>—IP precedence value. The range is 0 to 7. • <i>min-threshold</i>—the minimum threshold in packets. The range is 1 to 32768. When the average queue size reaches the minimum threshold, WRED randomly drops some packets with the specified precedence value. • <i>max-threshold</i>—the maximum threshold in packets. The range is 1 to 32768. When the average queue size exceeds the maximum threshold, WRED drops all packets with the specified precedence value. • <i>mark-prob-denominator</i>—the denominator for the fraction of packets dropped when the average queue size is at the maximum threshold. The range is 1 to 65535. For example, if the denominator is 512, one out of every 512 packets is dropped when the queue is at the maximum threshold. The default is 10; 1 out of every 10 packets is dropped at the maximum threshold.

Defaults

For all precedences, the *mark-prob-denominator* default is 10. The *min-threshold* default is 64 packets, and the *max-threshold* default is 128 packets.

The default *min-threshold* depends on the precedence as listed in [Table 2-16 on page 2-348](#). The *min-threshold* for IP precedence 0 corresponds to half of the *max-threshold*. The values for the remaining precedences fall between half the *max-threshold* and the *max-threshold* at evenly spaced intervals.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.
12.2(25)EY	Hierarchical service policies can be attached to inbound traffic received on an ES port.

Usage Guidelines

WRED is a congestion-avoidance mechanism that slows traffic by randomly dropping packets when congestion exists. WRED reduces the chances of tail drop by selectively dropping packets when the egress port begins to show signs of congestion. By dropping some packets early rather than waiting until the queue is full, WRED does not drop large numbers of packets at once.

Use the **random-detect precedence** command only in a hierarchical policy map attached to an ES port. You can use this command only in class-level classes.

You must configure the **bandwidth** or the **shape** policy-map class configuration command before you configure either the **queue-limit** or the **random-detect** policy-map class configuration command in a class policy.

You can define a class policy to use either tail drop or WRED packet drop by using either the **queue-limit** policy-map class configuration command or the **random-detect** policy-map class configuration command, respectively. You cannot use the **queue-limit** and **random-detect** commands in the same class policy, but they can be used in two class policies in the same policy map.

You cannot use the **bandwidth**, **queue-limit**, **random-detect**, and the **shape** policy-map class configuration commands with the **priority** policy-map class configuration command in the same class within the same policy map. However, you can use these commands in the same policy map.

You must enter the **random-detect precedence-based** command before specifying the values with the **random-detect precedence** *ip-precedence min-threshold max-threshold mark-prob-denominator* command.

If you want WRED to ignore the precedence when deciding which packets to drop, enter the **random-detect precedence** command with the same parameters for each precedence. Remember to use reasonable values for the minimum and maximum thresholds.

Set the *min-threshold* value high enough to maximize the link usages. If the minimum threshold is too low, packets might be dropped unnecessarily, and the transmission link is not fully used. The difference between the maximum threshold and the minimum threshold should be large enough to avoid global synchronization of TCP hosts. This can occur as multiple TCP hosts reduce their transmission rates. If the difference between the maximum and minimum thresholds is too small, many packets might be dropped at once, resulting in global synchronization.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Table 2-16 lists the default minimum threshold value for each IP Precedence.

Table 2-16 Default WRED Minimum Threshold Values

IP Precedence	WRED Minimum Threshold Value
0	9/18
1	10/18
2	11/18
3	12/18
4	13/18
5	14/18
6	15/18
7	16/18
RSVP	17/18

**Note**

The default WRED parameter values are based on the best available data. We recommend that you do not change the parameters from their default values unless you have decided that your applications would benefit from the changed values.

Examples

This example shows how to enable IP precedence-based WRED as a drop policy. It uses the IP precedence value 3 for class *c1*. The minimum threshold for IP precedence value 3 is 24, the maximum threshold is 40, and the mark-probability denominator is 512. The last command attaches the service policy to the port.

```
Switch(config)# class-map c1
Switch(config-cmap)# match ip precedence 3
Switch(config-cmap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# bandwidth 48
Switch(config-pmap-c)# random-detect precedence-based
Switch(config-pmap-c)# random-detect precedence 3 24 40 512
Switch(config-pmap-c)# exit
Switch(config-pmap)# end
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# service-policy output p1
```

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

Related Commands

Command	Description
bandwidth	Specifies or modifies the minimum bandwidth provided to a class belonging to a policy map attached to an ES port.
class	Specifies the name of the class whose traffic policy you want to create or change.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
priority	Enables the strict-priority queue and gives priority to a class of traffic belonging to a policy map attached to an ES port.
queue-limit	Configures the maximum threshold for tail drop in a policy map attached to an ES port.
random-detect	Enables WRED in a policy map attached to an ES port.
random-detect exponential-weighting-constant	Configures WRED exponential weight factor for the average queue-size calculation for the queue in a policy map attached to an ES port.
service-policy (policy-map class)	Creates a service policy as a quality of service (QoS) policy within a policy map.
shape	Enables traffic shaping in a policy map attached to an ES port.
show policy-map	Displays QoS policy maps.

rcommand

Use the **rcommand** user EXEC command to start a Telnet session and to execute commands on a cluster member switch from the cluster command switch. To end the session, enter the **exit** command.

rcommand { *n* | **commander** | **mac-address** *hw-addr* }

Syntax Description	<i>n</i>	Provide the number that identifies a cluster member. The range is 0 to 15.
	commander	Provide access to the cluster command switch from a cluster member switch.
	mac-address <i>hw-addr</i>	MAC address of the cluster member switch.

Command Modes	User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines

This command is available only on the cluster command switch.

If the switch is the cluster command switch but the cluster member switch *n* does not exist, an error message appears. To obtain the switch number, enter the **show cluster members** privileged EXEC command on the cluster command switch.

You can use this command to access a cluster member switch from the cluster command-switch prompt or to access a cluster command switch from the member-switch prompt.

For Catalyst 2900 XL, 3500 XL, 2950, 2970, 3550, and 3750 switches and Catalyst 3750 Metro switches, the Telnet session accesses the member-switch command-line interface (CLI) at the same privilege level as on the cluster command switch. For example, if you execute this command at user level on the cluster command switch, the cluster member switch is accessed at user level. If you use this command on the cluster command switch at privileged level, the command accesses the remote device at privileged level. If you use an intermediate enable-level lower than *privileged*, access to the cluster member switch is at user level.

For Catalyst 1900 and 2820 switches running standard edition software, the Telnet session accesses the menu console (the menu-driven interface) if the cluster command switch is at privilege level 15. If the cluster command switch is at privilege level 1, you are prompted for the password before being able to access the menu console. Cluster command switch privilege levels map to the cluster member switches running standard edition software as follows:

- If the cluster command switch privilege level is from 1 to 14, the cluster member switch is accessed at privilege level 1.
- If the cluster command switch privilege level is 15, the cluster member switch is accessed at privilege level 15.

The Catalyst 1900 and 2820 CLI is available only on switches running Enterprise Edition Software.

This command will not work if the vty lines of the cluster command switch have access-class configurations.

You are not prompted for a password because the cluster member switches inherited the password of the cluster command switch when they joined the cluster.

Examples

This example shows how to start a session with member 3. All subsequent commands are directed to member 3 until you enter the **exit** command or close the session.

```
Switch# rcommand 3
Switch-3# show version
Cisco Internet Operating System Software ...
...
Switch-3# exit
Switch#
```

Related Commands

Command	Description
show cluster members	Displays information about the cluster members.

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	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>12.1(14)AX</td><td>This command was introduced.</td></tr> </table>	Release	Modification	12.1(14)AX	This command was introduced.
Release	Modification				
12.1(14)AX	This command was introduced.				

Usage Guidelines

You can configure RSPAN VLANs only in config-VLAN mode (entered by using the **vlan** global configuration command), not the VLAN configuration mode entered by using the **vlan database** privileged EXEC command.

If VTP is enabled, the RSPAN feature is propagated by VLAN Trunking Protocol (VTP) for VLAN-IDs that are lower than 1005. If the RSPAN VLAN ID is in the extended range, you must manually configure intermediate switches (those in the RSPAN VLAN between the source switch and the destination switch).

Before you configure the RSPAN **remote-span** command, use the **vlan** (global configuration) command to create the VLAN.

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.

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 are made 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
	monitor session	Enables Switched Port Analyzer (SPAN) and RSPAN monitoring on a port and configures a port as a source or destination port.
	vtp (global configuration)	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 [{ **flash:**/*filename* | **ftp:**/*user:password@host/filename* | **nvr:**/*filename* | **r:**/*user@host/filename* | **tftp:**/*host/filename* }] [**validation none**]

Syntax Description	flash: / <i>filename</i>	(Optional) Specify that the database agent or the binding file is in the flash memory.
	ftp: / <i>user:password@host/filename</i>	(Optional) Specify that the database agent or the binding file is on an FTP server.
	nvr: / <i>filename</i>	(Optional) Specify that the database agent or the binding file is in the NVRAM.
	r: / <i>user@host/filename</i>	(Optional) Specify that the database agent or the binding file is on a Remote Control Protocol (RCP) server.
	tftp: / <i>host/filename</i>	(Optional) Specify that the database agent or the binding file is on a TFTP server.
	validation none	(Optional) Specify that the switch does not verify the cyclic redundancy check (CRC) for the entries in the binding file specified by the URL.

Defaults No default is defined.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(25)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 in the file:

```
Switch# renew ip dhcp snooping database validation none
```

To verify your settings, enter the **show ip dhcp snooping database** privileged EXEC command.

Related Commands	Command	Description
	ip dhcp snooping	Enables DHCP snooping on a VLAN.
	ip dhcp snooping binding	Configures the DHCP snooping binding database.
	show ip dhcp snooping database	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(40)SE	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
show interfaces rep detail	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

id <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 show interface interface-id rep detail 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.
preferred	Identify the VLAN blocking alternate port as the segment port on which you entered the rep segment segment-id preferred interface configuration command. Note Entering the preferred keyword does not ensure that the preferred port is the alternate port; it gives it preference over other similar ports.
vlan	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.
all	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

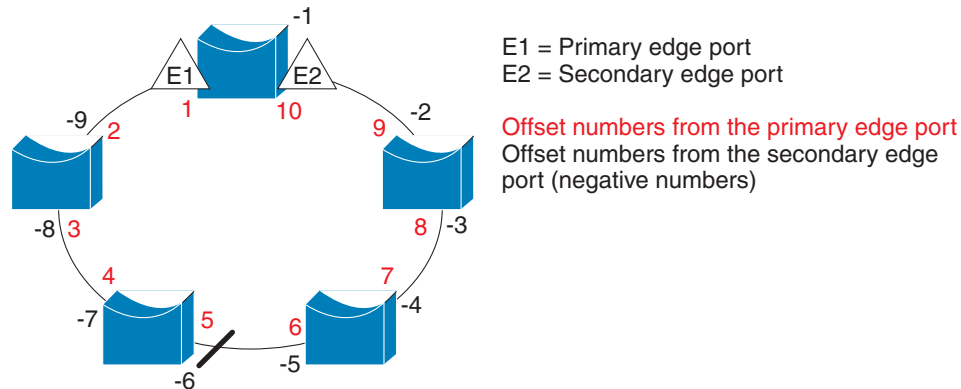
Release	Modification
12.2(40)SE	This command was introduced.

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



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.

Examples

This example shows how to configure REP VLAN load balancing on the Switch B primary edge port (Gigabit Ethernet port 1/0/1) and to configure Gigabit Ethernet port 1/0/2 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 gigabitethernet1/0/1
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 gigabitethernet1/0/2
Switch (config-if)# rep block port 6 vlan 1-110
Switch (config-if)# end

Switch# show interface gigabitethernet1/0/2 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
rep preempt delay	Configures a waiting period after a segment port failure and recovery before REP VLAN load balancing is triggered.
rep preempt segment	Manually starts REP VLAN load balancing on a segment.
show interfaces rep detail	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 with 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

Syntax Description	<i>value</i>	The age-out time in milliseconds. The range is from 3000 ms to 10000 ms in 500 ms increments. The default is 5000 ms (5 seconds).

Defaults	The REP interface shuts down if it does not receive a hello message from a neighbor for 5000 ms.

Command Modes	Interface configuration

Command History	Release	Modification
	12.2(46)SE	This command was introduced.

Usage Guidelines	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 within the LSL age timer period. If no hellos are received within that time, the REP link is brought down.

Examples	This example shows how to configure the REP LSL age timer on a REP link to 7000 ms: <pre>Switch (config)# interface gigabitethernet1/0/2 Switch (config-if)# rep lsl-age-timer 7000 Switch (config-if)# exit</pre> You can verify the configured ageout time by entering the show interfaces rep detail privileged EXEC command.

Related Commands	Command	Description
	show interfaces rep [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	<i>seconds</i> 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(40)SE	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.
	Do not configure VLAN load balancing on an interface that carries Ethernet over multiprotocol label switching (EoMPLS) traffic. VLAN load balancing across the REP ring might cause some of the EoMPLS traffic to not be forwarded.

Examples	This example shows how to configure REP preemption time delay of 100 seconds on the primary edge port:
	<pre>Switch (config)# interface gigabitethernet1/0/1 Switch (config-if)# rep preempt delay 100 Switch (config-if)# exit</pre>

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

Related Commands	Command	Description
	rep block port	Configures VLAN load balancing.
	show interfaces rep [detail]	Displays REP configuration and status for all interfaces or the 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(40)SE	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
rep block port	Configures VLAN load balancing.
show interfaces rep [detail]	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.
edge	(Optional) Identify the interface as one of the two REP edge ports. Entering the edge keyword without the primary keyword configures the port as the secondary edge port.
no-neighbor	(Optional) Configure a segment edge with no external REP neighbor.
primary	(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.
preferred	(Optional) Specify that the port is the preferred alternate port or the preferred port for VLAN load balancing.
Note	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(40)SE	This command was introduced.
12.2(50)SE	The no-neighbor 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

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 is supported on EtherChannels, but not on an individual port that belongs to an EtherChannel.

- 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 gigabitethernet1/0/1
Switch (config-if)# rep segment 100
```

This example shows how to enable REP on a port and identify the port as the REP primary edge port:

```
Switch (config)# interface gigabitethernet1/0/2
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 identify the port as the REP secondary edge port:

```
Switch (config)# interface gigabitethernet1/0/2
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
show interfaces rep [detail]	Displays REP configuration and status for all interfaces or the specified interface.
show rep topology [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	interface <i>interface-id</i>	Identify a physical interface or port channel to receive STCNs.
	segment <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).
	stp	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(40)SE	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 a REP edge port to send STCNs to segments 25 to 50:

```
Switch (config)# interface gigabitethernet1/0/2
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
show interfaces rep [detail]	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# config 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
show ip dhcp pool	Displays the DHCP address pools.

rmon collection stats

Use the **rmon collection stats** interface configuration command to collect Ethernet group statistics, which include utilization 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.



Note

Though visible in the command-line help, the **rmon native** and **rmon promiscuous** commands are not supported.

Defaults

The RMON statistics collection is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The RMON statistics collection command is based on hardware counters.

Examples

This example shows how to collect RMON statistics for the owner *root* on a port:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# rmon collection stats 2 owner root
```

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

Related Commands

Command	Description
show rmon statistics	Displays RMON statistics.
	For syntax information, select Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > System Management Commands > RMON Commands .

sdm prefer

Use the **sdm prefer** global configuration command to configure the template used in the Switch Database Management (SDM) resource allocation. You can use a template to allocate system resources to best support the features being used in your application. Use a template to provide maximum system utilization for routing or for VLAN configuration. Use the **no** form of this command to return to the default template.

sdm prefer { default | routing | vlan }

no sdm prefer



Note

Though visible in the command-line help string, the **dual-ipv4-and-ipv6** keywords are not supported.

Syntax Description

default	Set the switch to use the default template to balance resources among features.
routing	Provide maximum system utilization for unicast routing. You would typically use this template for a router or aggregator in the middle of a network. Note This template does not support policy-based routing.
vlan	Provide maximum system utilization for VLANs. This template maximizes system resources for use as a Layer 2 switch with no routing.

Defaults

The default template provides a balance to all features.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.
12.2(25)EY	The routing-pbr keywords for configuring the policy-based routing template were removed. This template is no longer required for policy-based routing.

Usage Guidelines

You must reload the switch for the configuration to take effect.

Use the **sdm prefer vlan** global configuration command only on switches intended for Layer 2 switching with no routing. When you use the VLAN template, no system resources are reserved for routing entries, and any routing is done through software. This overloads the CPU and severely degrades routing performance.

Do not use the routing template if you do not have routing enabled on your switch. Entering the **sdm prefer routing** global configuration command prevents other features from using the memory allocated to unicast routing in the routing template.

Table 2-17 lists the approximate number of each resource supported in each of the three templates for a switch. The first eight rows in the tables (unicast MAC addresses through security access control entries [ACEs]) represent approximate hardware boundaries set when you select a template. If a section of a hardware resource is full, all processing overflow is sent to the CPU, seriously impacting switch performance. The last row is a guideline used to calculate hardware resource consumption related to the other resource parameters.

Table 2-17 Approximate Number of Feature Resources Allowed by Each Template

Resource	Templates		
	Default	Routing	VLAN
Unicast MAC addresses	6 K	3 K	12 K
Internet Group Management Protocol (IGMP) groups and multicast routes	1 K	1 K	1 K
Unicast routes	8 K	11 K	0
• Directly connected hosts	6 K	3 K	0
• Indirect routes	2 K	8 K	0
Policy-based routing ACEs	0	512	0
Quality of service (QoS) classification ACEs	512	512	512
Security ACEs	1 K	1 K	1 K
Layer 2 VLANs	1 K	1 K	1 K

Examples

This example shows how to configure the routing template on a switch:

```
Switch(config)# sdm prefer routing
Switch(config)# exit
Switch# reload
```

This example shows how to change a switch template to the default template.

```
Switch(config)# sdm prefer default
Switch(config)# exit
Switch# reload
```

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

Related Commands

Command	Description
show sdm prefer	Displays the current SDM template in use or displays the templates that can be used, with 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*

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.
	ethernet	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(25)SEG	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)#
```

Related Commands	Command	Description
	show ethernet service instance	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 hold down the **Mode** button and interrupt the boot process while the switch is powering up and to assign a new password. Use the **no** form of this command to disable part of the password-recovery functionality. When the password-recovery mechanism is disabled, interrupting the boot process is allowed only if the user agrees to set the system back to the default configuration.

service password-recovery

no service password-recovery

Syntax Description	This command has no arguments or keywords.

Defaults	The password-recovery mechanism is enabled.

Command Modes	Global configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	As a system administrator, you can use the no service password-recovery command to disable some of the functionality of the password recovery feature by allowing an end user to reset a password only by agreeing to return to the default configuration.

To use the password-recovery procedure, a user with physical access to the switch holds down the Mode button while the unit powers up and for a second or two after the LED above port 1X goes off. When the button is released, the system continues with initialization. If the password-recovery mechanism is disabled, this message appears:

```
The password-recovery mechanism has been triggered, but
is currently disabled. Access to the boot loader prompt
through the password-recovery mechanism is disallowed at
this point. However, if you agree to let the system be
reset back to the default system configuration, access
to the boot loader prompt can still be allowed.
```

```
Would you like to reset the system back to the default configuration (y/n)?
```

If the user chooses not to reset the system back to the default configuration, the normal boot process continues, as if the **Mode** button had not been pressed. If you choose to reset the system back to the default configuration, the configuration file in flash memory is deleted, and the VLAN database file, *flash:vlan.dat* (if present), is deleted.

**Note**

If you use the **no service password-recovery** command to control end user access to passwords, we recommend that you save a copy of the config file in a location away from the switch in case the end user uses the password recovery procedure and sets the system to default values. Do not keep a backup copy of the config file on the switch.

If the switch is operating in VLAN Trunking Protocol (VTP) transparent mode, we recommend that you also save a copy of the vlan.dat file in a location away from the switch.

You can verify if password recovery is enabled or disabled by entering the **show version** privileged EXEC command.

Examples

This example shows how to disable password recovery 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
show version	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 a port or a switch virtual interface (SVI). Use the **no** form of this command to remove the policy map and port association.

service-policy {input | output} *policy-map-name*

no service-policy {input | output} *policy-map-name*

Syntax Description

input <i>policy-map-name</i>	Apply the specified single-level ingress policy map to a standard or to an enhanced-services (ES) port. Apply the specified hierarchical policy map to the input of an enhanced-services (ES) port or Etherchannel made of ES ports.
output <i>policy-map-name</i>	Apply the specified single-level or hierarchical policy map to the output of an ES port or EtherChannel.



Note

Though visible in the command-line help strings, the **history** keyword is not supported, and you should ignore the statistics it gathers.

Defaults

No policy maps are attached to the port.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.
12.2(25)EY	Hierarchical service policies can be attached to inbound or outbound traffic on an ES port. Nonhierarchical dual-level service policies can be attached to inbound traffic received on a switch virtual interface (SVI).
12.2(25)SE	Hierarchical service policies can be attached to an EtherChannel with no ports or with one or both ES ports

Usage Guidelines

Only one policy map per port is supported. With standard QoS, you can attach one nonhierarchical service policy to the input of a standard physical port, to an SVI, or to an ES port. You can also attach one ingress hierarchical dual-level service policy per SVI. With hierarchical QoS, you can attach one ingress hierarchical service policy and one egress hierarchical service policy per ES port. You can also attach a hierarchical service policy to an EtherChannel with no ports or with one or both ES ports

Use the **service-policy output** *policy-map-name* command only in an egress policy map attached to an ES port. You cannot apply an egress policy to a standard port.

In software releases earlier than Cisco IOS Release 12.2(25)EY, policy maps can be configured only on physical ports. In Cisco IOS Release 12.2(25)EY or later, policy maps can be configured on physical ports or on SVIs. When VLAN-based quality of service (QoS) is disabled by using the **no mls qos vlan-based** interface configuration command on a physical port, you can configure a port-based policy map on the port. If VLAN-based QoS is enabled by using the **mls qos vlan-based** interface configuration command on a physical port, the switch removes the previously configured port-based policy map. After a dual-level policy map is configured and applied on an SVI, the interface-level policy map takes effect on the interface.

In software releases earlier than Cisco IOS Release 12.2(25)EY, you can apply a policy map only to the input of a physical port. In Cisco IOS Release 12.2(25)EY or later, you can apply a policy map to the input of a physical port or an SVI.

In Cisco IOS Release 12.2(35)SE or later, you can attach a hierarchical policy map to an EtherChannel made of ES ports.

When applying an ingress nonhierarchical policy map to a physical interface or an SVI or when applying an egress hierarchical policy map to a ES port, classification using a port trust state (for example, **mls qos trust [cos | dscp | ip-precedence]**) and a policy map (for example, **service-policy input policy-map-name**) are mutually exclusive. The last one configured overwrites the previous configuration. However, if you are applying an ingress hierarchical policy to an ES port that includes the **set** policy-map class configuration command or policing actions in a two-rate policer, the switch automatically applies a port trust state to the ES port. For example, if you configure the **set cos new-cos** command, the switch automatically configures the interface to trust CoS.

You can attach single-level policy maps as input policies on a standard ports or as input or output policies on ES ports. You cannot apply a single-level policy map to an egress standard port.

You can attach hierarchical policy maps as input or output policies on ES ports or ES EtherChannels. You cannot attach hierarchical policy maps to standard ports.

In releases earlier than Cisco IOS Release 12.2(35)SE, the switch does not support attaching a service policy to a logical interface (such as an EtherChannel). In these releases, you must configure quality of service (QoS) classification, policing, mapping, and queueing on the individual physical ports that comprise the EtherChannel. In Cisco IOS Release 12.2(35) or later, you can configure hierarchical policy maps on EtherChannels made of ES ports

Examples

This example shows how to apply a policy map to the input of a standard port:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# service-policy input plcmap1
```

This example shows how to apply a policy map to the output of an ES port:

```
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# service-policy output plcmap3
```

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

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.

Command	Description
show policy-map	Displays QoS policy maps.
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.

service-policy (policy-map class)

Use the **service-policy** policy-map class configuration command to create a service policy that is a quality of service (QoS) policy within a policy map (called a hierarchical service policy). Use the **no** form of this command to disable the service policy within a policy map.

service-policy *policy-map-name*

no service-policy *policy-map-name*

Syntax Description	<i>policy-map-name</i>	Name of the policy map.

Defaults	No service policies maps are defined.

Command Modes	Policy-map class configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.
	12.2(25)EY	Hierarchical service policies can be attached to inbound traffic received on an ES port or a switch virtual interface (SVI).

Usage Guidelines	Use the service-policy command only in a hierarchical policy map attached to an enhanced-services (ES) port. This command is valid in policy maps at any level of the hierarchy.
	You can create a hierarchy by associating a class-level policy map with a VLAN-level policy map, by associating that VLAN-level policy map with a physical-level policy map, and by attaching the physical-level policy map to an ES port. You can omit hierarchical levels, but the order of the levels (class level, VLAN level, and then the physical level) must be preserved.
	If you use the bandwidth policy-map class configuration command in a child policy, you also must use it in the parent policy.
	If you enter this command in policy-map class configuration mode, you return to policy-map configuration mode by using the exit command. To return to privileged EXEC mode, use the end command.

Examples	This example shows how to create a hierarchical service policy in the service policy called <i>parent</i> :

```
Switch(config)# policy-map child
Switch(config-pmap)# class voice
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map parent
Switch(config-pmap)# class class1
Switch(config-pmap-c)# shape average 10000000
Switch(config-pmap-c)# service-policy child
```

This example shows how to create a hierarchical service policy in which all levels are present. This configuration associates a class-level policy map with a VLAN-level policy map, associates the VLAN-level policy map with a physical-level policy map, and attaches the physical-level policy map to a port.

```
Switch(config)# class-map my-class
Switch(config-cmap)# match ip precedence 1
Switch(config-cmap)# exit
Switch(config)# class-map my-logical-class
Switch(config-cmap)# match vlan 5
Switch(config-cmap)# exit
Switch(config)# policy-map my-class-policy
Switch(config-pmap)# class my-class
Switch(config-pmap-c)# set precedence 2
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map my-logical-policy
Switch(config-pmap)# class my-logical-class
Switch(config-pmap-c)# shape average 400000000
Switch(config-pmap-c)# service-policy my-class-policy
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map my-physical-policy
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 500000000
Switch(config-pmap-c)# service-policy my-logical-policy
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1/1
Switch(config)# service-policy input my-physical-policy
```

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

Related Commands	Command	Description
	bandwidth	Specifies or modifies the minimum bandwidth provided to a class belonging to a policy map attached to an ES port.
	class	Specifies the name of the class whose traffic policy you want to create or change.
	policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
	priority	Enables the strict-priority queue and gives priority to a class of traffic belonging to a policy map attached to an ES port.
	queue-limit	Configures the maximum threshold for tail drop in a policy map attached to an ES port.
	random-detect	Configures Weighted Random Early Detection (WRED) in a policy map attached to an ES port.
	shape	Enables traffic shaping in a policy map attached to an ES port.
	show policy-map	Displays QoS policy maps.

set

Use the **set** policy-map class configuration command to classify IP traffic by setting a class of service (CoS), a Differentiated Services Code Point (DSCP), an IP-precedence, or the multiprotocol label switching (MPLS) experimental (EXP) bits in the packet. Use the **no** form of this command to remove the traffic classification.

set {**cos** *new-cos* | [**ip**] {**dscp** *new-dscp* | **precedence** *new-precedence*} | **mpls experimental** *exp-number*}

no set **cos** *new-cos* | **ip** {**dscp** *new-dscp* | **precedence** *new-precedence*} | **mpls experimental** *exp-number*}

Syntax Description		
cos <i>new-cos</i>		New CoS value assigned to the classified traffic. The range is 0 to 7.
ip dscp <i>new-dscp</i>		New DSCP value assigned to the classified traffic. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value. The specified value sets the type of service (ToS) byte in the packet header.
ip precedence <i>new-precedence</i>		New IP-precedence value assigned to the classified traffic. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value. The specified value sets the precedence bit in the IP header.
mpls experimental <i>exp-number</i>		New MPLS experimental value assigned to the classified traffic. The range is 0 to 7. The specified value sets the MPLS experimental 3-bit field in the packet header.

Defaults No traffic classification is defined.

Command Modes Policy-map class configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.
	12.2(25)EY	Hierarchical service policies can be attached to inbound traffic received on an ES port.

Usage Guidelines You can use the **set** command only in class-level classes.

The **set dscp** *new-dscp* and the **set precedence** *new-precedence* commands are the same as the **set ip dscp** *new-dscp* and the **set ip precedence** *new-precedence* commands.

For the **set dscp** *new-dscp* or the **set precedence** *new-precedence* command, you can enter a mnemonic name for a commonly used value. For example, you can enter the **set dscp af11** command, which is the same as entering the **set dscp 10** command. You can enter the **set precedence critical** command, which is the same as entering the **set precedence 5** command. For a list of supported mnemonics, enter the **set dscp ?** or the **set precedence ?** command to see the command-line help strings.

You can configure the **set cos** *new-cos*, **set dscp** *new-dscp*, **set precedence** *new-precedence*, or the **set mpls experimental** *exp-number* command in an ingress and an egress policy map attached to an enhanced-services (ES) port. You can configure only the **set dscp** *new-dscp* or the **set precedence** *new-precedence* command in an ingress nonhierarchical policy map attached to a standard SVI or an ES port.

If an ingress hierarchical policy map includes **set cos** *new-cos*, the **set dscp** *new-dscp*, or the **set precedence** *new-precedence* command, the switch automatically applies the port trust state to the ES port. The switch applies the port trust state to all inbound traffic on the ES port, including traffic that does not match the traffic class. For example, if you enter the **set cos** *new-cos* command, the switch automatically configures the interface to trust CoS.

In an ingress policy map, you cannot combine Layer 2 and Layer 3 **set** actions because the port can trust only one value in the inbound packet. For example, the switch does not support this policy map:

```
policy-map p1
  class cos1
    police cir per 10 conform-action set-cos-transmit 3
    set dscp af22
```

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 *p1* with CoS values assigned to different traffic types. Class maps for *voice* and *video-data* have already been created.

```
Switch(config)# policy-map p1
Switch(config-pmap)# class voice
Switch(config-pmap-c)# set cos 1
Switch(config-pmap)# exit
Switch(config-pmap)# class video-data
Switch(config-pmap-c)# set cos 2
Switch(config-pmap)# exit
```

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

Related Commands

Command	Description
class	Specifies the name of the class whose traffic policy you want to create or change.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map	Displays quality of service (QoS) policy maps.
trust	Defines a trust state for traffic class.

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
	12.1(14)AX	This command was introduced.

Usage Guidelines When you use the **setup** command, make sure that you have this information:

- IP address and network mask
- Password strategy for your environment
- Whether the switch will be used as the cluster command switch and the cluster name

When you enter the **setup** command, an interactive dialog, called the System Configuration Dialog, appears. It guides you through the configuration process and prompts you for information. The values shown in brackets next to each prompt are the default values last set by using either the **setup** command facility or the **configure** privileged EXEC command.

Help text is provided for each prompt. To access help text, press the question mark (?) key at a prompt.

To return to the privileged EXEC prompt without making changes and without running through the entire System Configuration Dialog, press **Ctrl-C**.

When you complete your changes, the setup program shows you the configuration command script that was created during the setup session. You can save the configuration in NVRAM, return to the setup program without saving, or return to the command-line prompt without saving the configuration.

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 [<Use current 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? [yes]: **yes**

Community string [public]:

Current interface summary

Interface	IP-Address	OK?	Method	Status	Pro
Vlan1	10.1.2.3	YES	NVRAM	up	up
Vlan100	unassigned	YES	NVRAM	down	down
Vlan150	unassigned	YES	NVRAM	down	down
Vlan901	unassigned	YES	NVRAM	down	down
FastEthernet1/0/1	unassigned	YES	unset	up	up
FastEthernet1/0/2	111.1.1.1	YES	NVRAM	up	up

<output truncated>

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*

Class A network is 10.0.0.0, 8 subnet bits; mask is /8

Would you like to enable as a cluster command switch? [yes/no]: **yes**

Enter cluster name: *cluster-name*

The following configuration command script was created:

```
hostname host-name
enable secret 5 $1$ZzDa$X8ic4TpKggQ5wOgQ/xqdz1
enable password enable-password
line vty 0 15
password terminal-password
snmp-server community public
!
no ip routing

!
interface Vlan1
no shutdown
ip address 10.1.2.3 255.0.0.0
!
interface Vlan100
shutdown
no ip address
!
interface Vlan150
```

```

shutdown
no ip address
!
interface Vlan901
shutdown
no ip address
!
interface FastEthernet1/0/1
!
interface FastEthernet1/0/2
shutdown
no ip address
!

```

<output truncated>

```

cluster enable cluster-name
!
end

```

- [0] Go to the IOS command prompt without saving this config.
 [1] Return back to the setup without saving this config.
 [2] Save this configuration to nvram and exit.

Enter your selection [2]:

Related Commands

Command	Description
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.
show version	Displays version information for the hardware and firmware.

setup express

Use the **setup express** global configuration command to enable Express Setup mode. Use the **no** form of this command to disable Express Setup mode.

setup express

no setup express

Syntax Description	This command has no arguments or keywords.

Defaults	Express Setup is enabled.

Command Modes	Global configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	When Express Setup is enabled on a new (unconfigured) switch, pressing the Mode button for 2 seconds activates Express Setup. You can access the switch through an Ethernet port by using the IP address 10.0.0.1 and then can configure the switch with the web-based Express Setup program or with the CLI-based setup program.

When you press the Mode button for 2 seconds on a configured switch, the LEDs next to the Mode button start blinking. If you press the Mode button for a total of 10 seconds, the switch configuration is deleted, and the switch reboots. The switch can then be configured like a new switch, either through the web-based Express Setup program or the CLI-based setup program.

**Note**

As soon as you make any change to the switch configuration (including entering *no* at the beginning of the CLI-based setup program), configuration by Express Setup is no longer available. You can only run Express Setup again by pressing the Mode button for 10 seconds. This deletes the switch configuration and reboots the switch.

If Express Setup is active on the switch, entering the **write memory** or **copy running-configuration startup-configuration** privileged EXEC commands deactivates Express Setup. The IP address 10.0.0.1 is no longer valid on the switch, and your connection using this IP address ends.

The primary purpose of the **no setup express** command is to prevent someone from deleting the switch configuration by pressing the Mode button for 10 seconds.

Examples

This example shows how to enable Express Setup mode:

```
Switch(config)# setup express
```

You can verify that Express Setup mode is enabled by pressing the Mode button:

- On an unconfigured switch, the mode LEDs turn solid green after 3 seconds.
- On a configured switch, the mode LEDs begin blinking after 2 seconds and turn solid green after 10 seconds.

**Caution**

If you hold the Mode button down for a total of 10 seconds, the configuration is deleted, and the switch reboots.

This example shows how to disable Express Setup mode:

```
Switch(config)# no setup express
```

You can verify that Express Setup mode is disabled by pressing the Mode button. The mode LEDs do not turn solid green *or* begin blinking if Express Setup mode is not enabled on the switch.

Related Commands

Command	Description
show setup express	Displays if Express Setup mode is active.

shape

Use the **shape** policy-map class configuration command to enable traffic shaping in a hierarchical policy map attached to an enhanced-services (ES) port. Traffic shaping limits the data transmission rate. Use the **no** form of this command to return to the default setting.

shape average *cir-bps*

no shape average

Syntax Description

average	Enable average-rate traffic shaping.
<i>cir-bps</i>	Committed information rate, the bit rate that traffic is shaped to, in bps. This is the access bit rate that you contract with your service provider or the service levels that you intend to maintain. The range is 64000 to 2000000000 bps. Allocate the shaped rate in 100-kbps increments; otherwise, the software rounds down the rate to the nearest 100-kbps increment.

Defaults

Average-rate traffic shaping is disabled.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.
12.2(25)EY	Hierarchical service policies can be attached to inbound traffic received on an ES port.

Usage Guidelines

Use the **shape** command only in a hierarchical policy map attached to an ES port. This command is valid in policy maps at any level of the hierarchy.

Shaping is the process of delaying out-of-profile packets in queues so that they conform to a specified profile. Shaping is distinct from policing. Policing drops packets that exceed a configured threshold, but shaping buffers packets so that traffic remains within the threshold. Shaping offers greater smoothness in handling traffic than policing.

You must configure the **bandwidth** or the **shape** policy-map class configuration command before you configure either the **queue-limit** or the **random-detect** policy-map class configuration command in a class policy.

You cannot use the **bandwidth**, **queue-limit**, **random-detect**, and the **shape** policy-map class configuration commands with the **priority** policy-map class configuration command in the same class within the same policy map. However, you can use these commands in the same policy map.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

The switch follows these rules when allocating bandwidth for VLAN-level and class-level classes:

- Shaping restricts the bandwidth available to VLAN-level classes. The shaping rate configured in the physical-level policy map becomes the total bandwidth available to all VLAN-level classes.
- For VLAN-level and class-level classes, the shaping rate becomes the available bandwidth if the bandwidth is not specified for that class.
- For VLAN-level and class-level classes, the shaping rate must be greater or equal to the bandwidth allocated at that level.
- The total bandwidth for VLAN-level classes, including the class-default, cannot exceed the available bandwidth of the port.
- The total bandwidth for class-level classes, including the class-default, cannot exceed the available bandwidth at the parent VLAN level.
- At the VLAN level and at the class level, the configured bandwidth is summed for all the children. If the summed bandwidth is less than the available bandwidth for the parent, the remaining bandwidth is distributed equally among the children.

Examples

This example shows how to limit the specified traffic class to a data transmission rate of 256 kbps:

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# shape average 256000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# service-policy output policy1
```

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

Related Commands

Command	Description
bandwidth	Specifies or modifies the minimum bandwidth provided to a class belonging to a policy map attached to an ES port.
class	Specifies the name of the class whose traffic policy you want to create or change.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
priority	Enables the strict-priority queue and gives priority to a class of traffic belonging to a policy map attached to an ES port.
queue-limit	Configures the maximum threshold for tail drop in a policy map attached to an ES port.
random-detect	Configures Weighted Random Early Detection (WRED) in a policy map attached to an ES port.
service-policy (policy-map class)	Creates a service policy as a quality of service (QoS) policy within a policy map.
show policy-map	Displays QoS policy maps.

show access-lists

Use the **show access-lists** privileged EXEC command to display access control lists (ACLs) configured on the switch.

show access-lists [*name* | *number* | **hardware counters** | **ipc**] [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description	
<i>name</i>	(Optional) Name of the ACL.
<i>number</i>	(Optional) ACL number. The range is 1 to 2699.
hardware counters	(Optional) Display global hardware ACL statistics for switched and routed packets.
ipc	(Optional) Display Interprocess Communication (IPC) protocol access-list configuration download information.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.



Note

Though visible in the command-line help strings, the **rate-limit** keywords are not supported.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	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.

This command also displays the MAC ACLs that are configured.

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

Examples This is an example of output from the **show access-lists** command:

```
Switch# show access-lists
Standard IP access list 1
 10 permit 1.1.1.1
 20 permit 2.2.2.2
 30 permit any
 40 permit 0.255.255.255, wildcard bits 12.0.0.0
Standard IP access list videowizard_1-1-1-1
```

```

10 permit 1.1.1.1
Standard IP access list videowizard_10-10-10-10
10 permit 10.10.10.10
Extended IP access list 121
10 permit ahp host 10.10.10.10 host 20.20.10.10 precedence routine
Extended IP access list CMP-NAT-ACL
Dynamic Cluster-HSRP deny ip any any
10 deny ip any host 19.19.11.11
20 deny ip any host 10.11.12.13
Dynamic Cluster-NAT permit ip any any
10 permit ip host 10.99.100.128 any
20 permit ip host 10.46.22.128 any
30 permit ip host 10.45.101.64 any
40 permit ip host 10.45.20.64 any
50 permit ip host 10.213.43.128 any
60 permit ip host 10.91.28.64 any
70 permit ip host 10.99.75.128 any
80 permit ip host 10.38.49.0 any

```

This is an example of output from the **show access-lists hardware counters** command:

```

Switch# show access-lists hardware counters
L2 ACL INPUT Statistics
Drop: All frame count: 0
Drop: All bytes count: 0
Bridge Only: All frame count: 0
Bridge Only: All bytes count: 0
Forwarding To CPU: All frame count: 0
Forwarding To CPU: All bytes count: 0

L3 ACL INPUT Statistics
Drop: All frame count: 0
Drop: All bytes count: 0
Bridge Only: All frame count: 0
Bridge Only: All bytes count: 0
Forwarding To CPU: All frame count: 0
Forwarding To CPU: All bytes count: 0
Forwarded: All frame count: 0
Forwarded: All bytes count: 0
Drop And Log: All frame count: 0
Drop And Log: All bytes count: 0
Bridge Only And Log: All frame count: 0
Bridge Only And Log: All bytes count: 0
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
Bridge Only: All frame count: 61
Bridge Only: All bytes count: 3904
Forwarding To CPU: All frame count: 0
Forwarding To CPU: All bytes count: 0

<output truncated>

```

This is an example of output from the **show access-lists ipc** command:

```
Switch# show access-lists ipc
LC Access List Config Updates Rcvd
Standard Access Lists rcvd      : 0
Simple Named Access Lists rcvd  : 0
Extended Access Lists rcvd      : 0
Extended Named Access Lists rcvd : 0
Rate-Limit Access Lists rcvd    : 0
Delete one Access List rcvd     : 0
```

Related Commands	Command	Description
	access-list	Configures a standard or extended numbered access list on the switch. For syntax information, select Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands .
	ip access list	Configures a named IP access list on the switch. For syntax information, select Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands .
	mac access-list extended	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 TFTP protocol.

show archive status [{ **begin** | **exclude** | **include** } *expression*]

Syntax Description	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.2(25)EY	This command was introduced.

Usage Guidelines	If you use the archive download-sw privileged EXEC command to download an image to a TFTP server, the output of the archive download-sw command shows the status of the download.
	If you do not have a TFTP server, you can use the Cluster Management Suite (CMS) to download the image by using the HTTP protocol. The show archive status command shows the progress of the download.
	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

Examples	These are examples of output from the show archive status command:

```
Switch# show archive status
IDLE: No upgrade in progress
```

```
Switch# show archive status
LOADING: Upgrade in progress
```

```
Switch# show archive status
EXTRACT: Extracting the image
```

```
Switch# show archive status
VERIFY: Verifying software
```

```
Switch# show archive status
RELOAD: Upgrade completed. Reload pending
```

Related Commands	Command	Description
	archive download-sw	Downloads a new image from a TFTP server to the switch.

show arp access-list

Use the **show arp access-list** user EXEC command to display detailed information about Address Resolution Protocol (ARP) access control lists (ACLs).

show arp access-list [*acl-name*] [| { **begin** | **exclude** | **include** } *expression*]

This command is available only if your switch is running the enhanced multilayer image (EMI).

Syntax Description	
<i>acl-name</i>	(Optional) Name of the ACL.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.2(25)EY	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

Examples	This is an example of output from the show arp access-list 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
```

Related Commands	Command	Description
	arp access-list	Defines an ARP ACL.
	deny (ARP access-list configuration)	Denies an ARP packet based on matches against the DHCP bindings.
	ip arp inspection filter vlan	Permits ARP requests and responses from a host configured with a static IP address.
	permit (ARP access-list configuration)	Permits an ARP packet based on matches against the DHCP bindings.

show auto qos

Use the **show auto qos** user EXEC command to display the initial configuration that is generated by the automatic quality of service (auto-QoS) feature.

show auto qos [**interface** *interface-id*] [**|** { **begin** | **exclude** | **include** } *expression*]

Syntax Description

interface <i>interface-id</i>	(Optional) Display auto-QoS information for the specified port or for all ports.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

In releases earlier than Cisco IOS Release 12.2(25)EY, the **show auto qos** [**interface** *interface-id*] command output shows the initial generated auto-QoS configuration.

In Cisco IOS Release 12.2(25)EY or later, the **show auto qos** command output shows only the auto-QoS command entered on each interface. The **show auto qos interface** *interface-id* command output shows the auto-QoS command entered on a specific interface.

Use the **show running-config** privileged EXEC command to display the auto-QoS configuration and the user modifications.

On an enhanced-services (ES) port, the **srr-queue bandwidth shape** interface configuration command is not part of the generated **auto qos voip** command list.

To display information about the QoS configuration that might be affected by auto-QoS, use one of these commands:

- **show mls qos**
- **show mls qos maps cos-dscp**
- **show mls qos interface** *interface-id* [**buffers** | **queueing**]
- **show mls qos maps** [**cos-dscp** | **cos-input-q** | **cos-output-q** | **dscp-cos** | **dscp-input-q** | **dscp-output-q**]
- **show mls qos input-queue**
- **show running-config**

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

Examples

This is an example of output from the **show auto qos** command after the **auto qos voip cisco-phone** and the **auto qos voip cisco-softphone** interface configuration commands are entered:

```
Switch> show auto qos
GigabitEthernet1/0/1
auto qos voip cisco-softphone
```

```
GigabitEthernet1/0/2
auto qos voip cisco-phone
```

This is an example of output from the **show auto qos interface interface-id** command when the **auto qos voip cisco-phone** interface configuration command is entered:

```
Switch> show auto qos interface gigabitethernet 1/0/1
GigabitEthernet1/0/1
auto qos voip cisco-phone
```

This is an example of output from the **show running-config** privileged EXEC command when the **auto qos voip cisco-phone** and the **auto qos voip cisco-softphone** interface configuration commands are entered:

```
Switch# show running-config
Building configuration...
...
mls qos map policed-dscp 24 26 46 to 0
mls qos map cos-dscp 0 8 16 26 32 46 48 56
mls qos srr-queue input bandwidth 90 10
mls qos srr-queue input threshold 1 8 16
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 67 33
mls qos srr-queue input cos-map queue 1 threshold 2 1
mls qos srr-queue input cos-map queue 1 threshold 3 0
mls qos srr-queue input cos-map queue 2 threshold 1 2
mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7
mls qos srr-queue input cos-map queue 2 threshold 3 3 5
mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 3 32
mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48
mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56
mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 5
mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 2 4
mls qos srr-queue output cos-map queue 4 threshold 2 1
mls qos srr-queue output cos-map queue 4 threshold 3 0
mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39
mls qos srr-queue output dscp-map queue 4 threshold 1 8
mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7
mls qos queue-set output 1 threshold 1 100 100 100 100
mls qos queue-set output 1 threshold 2 75 75 75 250
mls qos queue-set output 1 threshold 3 75 150 100 300
mls qos queue-set output 1 threshold 4 50 100 75 400
mls qos queue-set output 2 threshold 1 100 100 100 100
```

```

mls qos queue-set output 2 threshold 2 35 35 35 35
mls qos queue-set output 2 threshold 3 55 82 100 182
mls qos queue-set output 2 threshold 4 90 250 100 400
mls qos queue-set output 1 buffers 15 20 20 45
mls qos queue-set output 2 buffers 24 20 26 30
mls qos
...
!
class-map match-all AutoQoS-VoIP-RTP-Trust
  match ip dscp ef
class-map match-all AutoQoS-VoIP-Control-Trust
  match ip dscp cs3  af31
!
policy-map AutoQoS-Police-SoftPhone
  class AutoQoS-VoIP-RTP-Trust
    set dscp ef
    police 320000 8000 exceed-action policed-dscp-transmit
  class AutoQoS-VoIP-Control-Trust
    set dscp cs3
    police 32000 8000 exceed-action policed-dscp-transmit
!
...
!
interface GigabitEthernet1/0/1
  switchport mode access
  switchport port-security maximum 400
  service-policy input AutoQoS-Police-SoftPhone
  speed 100
  duplex half
  srr-queue bandwidth share 10 10 60 20
  srr-queue bandwidth shape 10 0 0 0
  auto qos voip cisco-softphone
!
interface GigabitEthernet1/0/2
  switchport mode access
  switchport port-security maximum 1999
  speed 100
  duplex full
  srr-queue bandwidth share 10 10 60 20
  srr-queue bandwidth shape 10 0 0 0
  mls qos trust device cisco-phone
  mls qos trust cos
  auto qos voip cisco-phone
!
<output truncated>

```

This is an example of output from the **show auto qos interface *interface-id*** command when the **auto qos voip cisco-phone** interface configuration command is entered:

```

Switch> show auto qos interface fastethernet1/0/2
FastEthernet1/0/2
auto qos voip cisco-phone

```

These are examples of output from the **show auto qos** command when auto-QoS is disabled on the switch:

```

Switch> show auto qos
AutoQoS not enabled on any interface

```

These are examples of output from the **show auto qos interface *interface-id*** command when auto-QoS is disabled on an interface:

```

Switch> show auto qos interface gigabitethernet1/0/1
AutoQoS is disabled

```

Related Commands

Command	Description
auto qos voip	Automatically configures QoS for VoIP within a QoS domain.
debug auto qos	Enables debugging of the auto-QoS feature.

show boot

Use the **show boot** privileged EXEC command to display the settings of the boot environment variables.

show boot [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

Examples	This is an example of output from the show boot command. Table 2-18 describes each field in the display.

```
Switch# show boot
BOOT path-list       : flash:c3750-i9-mz
Config file          : flash:/config.text
Private Config file  : flash:/private-config.text
Enable Break         : no
Manual Boot          : yes
HELPER path-list     :
```

Table 2-18 *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 the software uses to read and write a nonvolatile copy of the system configuration.
Private Config file	Displays the filename that the software uses to read and write a nonvolatile copy of the system configuration.
Enable Break	Displays whether a break during booting is enabled or disabled. If it is set to yes, on, or 1, you can interrupt the automatic boot process by pressing the Break key on the console after the flash file system is initialized.
Manual Boot	Displays whether the switch automatically or manually boots. If it is set to no or 0, the boot loader attempts to automatically boot 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.

**Note**

Though visible in the display, the Auto upgrade field is not supported.

Related Commands

Command	Description
boot config-file	Specifies the filename that the software uses to read and write a nonvolatile copy of the system configuration.
boot enable-break	Enables interrupting the automatic boot process.
boot manual	Enables manually booting the switch during the next boot cycle.
boot private-config-file	Specifies the filename that software uses to read and write a nonvolatile copy of the private configuration.
boot system	Specifies the image to load during the next boot cycle.

show class-map

Use the **show class-map** user EXEC command to display quality of service (QoS) class maps, which define the match criteria to classify traffic.

show class-map [*class-map-name*] [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description

<i>class-map-name</i>	(Optional) Display the contents of the specified class map.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show class-map** command:

```
Switch> show class-map
Class Map match-all videowizard_10-10-10-10 (id 2)
  Match access-group name videowizard_10-10-10-10

Class Map match-any class-default (id 0)
  Match any
Class Map match-all dscp5 (id 3)
  Match ip dscp 5
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
match (class-map configuration)	Defines the match criteria for a class map.

show cluster

Use the **show cluster** user EXEC command to display the cluster status and a summary of the cluster to which the switch belongs. This command can be entered on the cluster command switch and cluster member switches.

show cluster [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	If you enter this command on a switch that is not a cluster member, the error message <code>Not a management cluster member</code> appears.
	On a cluster member switch, this command displays the identity of the cluster command switch, the switch member number, and the state of its connectivity with the cluster command switch.
	On a cluster command switch, this command displays the cluster name and the total number of members. It also shows the cluster status and time since the status changed. If redundancy is enabled, it displays the primary and secondary command-switch information.
	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

Examples	This is an example of output when the show cluster command is entered on the active cluster command switch:

```
Switch> show cluster
Command switch for cluster "Ajang"
Total number of members:      7
Status:                      1 members are unreachable
Time since last status change: 0 days, 0 hours, 2 minutes
Redundancy:                   Enabled
    Standby command switch: Member 1
    Standby Group:            Ajang_standby
    Standby Group Number:    110
Heartbeat interval:           8
Heartbeat hold-time:          80
Extended discovery hop count: 3
```

This is an example of output when the **show cluster** command is entered on a cluster member switch:

```
Switch1> show cluster
Member switch for cluster "hapuna"
  Member number:          3
  Management IP address:   192.192.192.192
  Command switch mac address: 0000.0c07.ac14
  Heartbeat interval:      8
  Heartbeat hold-time:     80
```

This is an example of output when the **show cluster** command is entered on a cluster member switch that is configured as the standby cluster command switch:

```
Switch> show cluster
Member switch for cluster "hapuna"
  Member number:          3 (Standby command switch)
  Management IP address:   192.192.192.192
  Command switch mac address: 0000.0c07.ac14
  Heartbeat interval:      8
  Heartbeat hold-time:     80
```

This is an example of output when the **show cluster** command is entered on the cluster command switch that has lost connectivity with member 1:

```
Switch> show cluster
Command switch for cluster "Ajang"
  Total number of members: 7
  Status:                  1 members are unreachable
  Time since last status change: 0 days, 0 hours, 5 minutes
  Redundancy:              Disabled
  Heartbeat interval:      8
  Heartbeat hold-time:     80
  Extended discovery hop count: 3
```

This is an example of output when the **show cluster** command is entered on a cluster member switch that has lost connectivity with the cluster command switch:

```
Switch> show cluster
Member switch for cluster "hapuna"
  Member number:          <UNKNOWN>
  Management IP address:   192.192.192.192
  Command switch mac address: 0000.0c07.ac14
  Heartbeat interval:      8
  Heartbeat hold-time:     80
```

Related Commands

Command	Description
cluster enable	Enables a command-capable switch as the cluster command switch, assigns a cluster name, and optionally assigns a member number to it.
show cluster candidates	Displays a list of candidate switches.
show cluster members	Displays information about the cluster members.

show cluster candidates

Use the **show cluster candidates** privileged EXEC command to display a list of candidate switches.

show cluster candidates [**detail** | **mac-address** *H.H.H.*] [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description	detail	(Optional) Display detailed information for all candidates.
	mac-address <i>H.H.H.</i>	(Optional) MAC address of the cluster candidate.
	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	This command is available only on the cluster command switch.
	If the switch is not a cluster command switch, the command displays an empty line at the prompt.
	The SN in the display means <i>switch member number</i> . If E appears in the SN column, it means that the switch is discovered through extended discovery. If E does not appear in the SN column, it means that the <i>switch member number</i> is the upstream neighbor of the candidate switch. The hop count is the number of devices the candidate is from the cluster command switch.
	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

Examples	This is an example of output from the show cluster candidates command:

```
Switch> show cluster candidates
                                     |---Upstream---|
MAC Address   Name           Device Type   PortIf   FEC Hops SN PortIf   FEC
00d0.7961.c4c0 StLouis-2    WS-C3750 -12T Gi1/0/1     2    1  Fa0/11
00d0.bbf5.e900 ldf-dist-128 WS-C3524-XL   Fa0/7     1    0  Fa0/24
00e0.1e7e.be80 1900_Switch  1900         3        0    1  Fa0/11
00e0.1e9f.7a00 Surfers-24   WS-C2924-XL   Fa0/5     1    0  Fa0/3
00e0.1e9f.8c00 Surfers-12-2 WS-C2912-XL   Fa0/4     1    0  Fa0/7
00e0.1e9f.8c40 Surfers-12-1 WS-C2912-XL   Fa0/1     1    0  Fa0/9
```

This is an example of output from the **show cluster candidates** command that uses the MAC address of a cluster member switch directly connected to the cluster command switch:

```
Switch> show cluster candidates mac-address 00d0.7961.c4c0
Device 'Tahiti-12' with mac address number 00d0.7961.c4c0
Device type:                cisco WS-C3750 -12T
```

show cluster candidates

```

Upstream MAC address: 00d0.796d.2f00 (Cluster Member 0)
Local port:          Gi1/0/1   FEC number:
Upstream port:       GI1/0/11  FEC Number:
Hops from cluster edge: 1
Hops from command device: 1

```

This is an example of output from the **show cluster candidates** command that uses the MAC address of a cluster member switch three hops from the cluster edge:

```

Switch> show cluster candidates mac-address 0010.7bb6.1cc0
Device 'Ventura' with mac address number 0010.7bb6.1cc0
Device type:          cisco WS-C2912MF-XL
Upstream MAC address: 0010.7bb6.1cd4
Local port:           Fa2/1   FEC number:
Upstream port:        Fa0/24  FEC Number:
Hops from cluster edge: 3
Hops from command device: -

```

This is an example of output from the **show cluster candidates detail** command:

```

Switch> show cluster candidates detail
Device 'Tahiti-12' with mac address number 00d0.7961.c4c0
Device type:          cisco WS-C3512-XL
Upstream MAC address: 00d0.796d.2f00 (Cluster Member 1)
Local port:           Fa0/3   FEC number:
Upstream port:        Fa0/13  FEC Number:
Hops from cluster edge: 1
Hops from command device: 2
Device '1900_Switch' with mac address number 00e0.1e7e.be80
Device type:          cisco 1900
Upstream MAC address: 00d0.796d.2f00 (Cluster Member 2)
Local port:           3       FEC number: 0
Upstream port:        Fa0/11  FEC Number:
Hops from cluster edge: 1
Hops from command device: 2
Device 'Surfers-24' with mac address number 00e0.1e9f.7a00
Device type:          cisco WS-C2924-XL
Upstream MAC address: 00d0.796d.2f00 (Cluster Member 3)
Local port:           Fa0/5   FEC number:
Upstream port:        Fa0/3   FEC Number:
Hops from cluster edge: 1
Hops from command device: 2

```

Related Commands

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

show cluster members

Use the **show cluster members** privileged EXEC command to display information about the cluster members.

show cluster members [*n* | **detail**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description	
<i>n</i>	(Optional) Number that identifies a cluster member. The range is 0 to 15.
detail	(Optional) Display detailed information for all cluster members.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines This command is available only on the cluster command switch.

If the cluster has no members, this command displays an empty line at the prompt.

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

Examples This is an example of output from the **show cluster members** command. The SN in the display means *switch number*.

```
Switch# show cluster members

SN MAC Address      Name              PortIf FEC Hops |---Upstream---|
0  0002.4b29.2e00 StLouis1          Fa0/13          0      0  0 Gi0/1          Up   (Cmdr)
1  0030.946c.d740 tal-switch-1      Fa0/13          1      0  1 Gi0/1          Up
2  0002.b922.7180 nms-2820          10              0      2  1 Fa0/18         Up
3  0002.4b29.4400 SanJuan2          Gi0/1           2      1  1 Fa0/11         Up
4  0002.4b28.c480 GenieTest         Gi0/2           2      1  1 Fa0/9          Up
```

This is an example of output from the **show cluster members** for cluster member 3:

```
Switch# show cluster members 3
Device 'SanJuan2' with member number 3
Device type:          cisco WS-C3750-12T
MAC address:          0002.4b29.4400
Upstream MAC address: 0030.946c.d740 (Cluster member 1)
Local port:           Gi1/0/1   FEC number:
Upstream port:        Gi1/0/11  FEC Number:
Hops from command device: 2
```

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

```
Switch# show cluster members detail
Device 'StLouis1' with member number 0 (Command Switch)
  Device type:      cisco WS-C3750-12T
  MAC address:      0002.4b29.2e00
  Upstream MAC address:
  Local port:              FEC number:
  Upstream port:           FEC Number:
  Hops from command device: 0
Device 'tal-switch-14' with member number 1
  Device type:      cisco WS-C3548-XL
  MAC address:      0030.946c.d740
  Upstream MAC address: 0002.4b29.2e00 (Cluster member 0)
  Local port:      Fa0/13  FEC number:
  Upstream port:   Gi0/1   FEC Number:
  Hops from command device: 1
Device 'nms-2820' with member number 2
  Device type:      cisco 2820
  MAC address:      0002.b922.7180
  Upstream MAC address: 0030.946c.d740 (Cluster member 1)
  Local port:      10      FEC number: 0
  Upstream port:   Fa0/18  FEC Number:
  Hops from command device: 2
Device 'SanJuan2' with member number 3
  Device type:      cisco WS-C3750-12T
  MAC address:      0002.4b29.4400
  Upstream MAC address: 0030.946c.d740 (Cluster member 1)
  Local port:      Gi1/0/1  FEC number:
  Upstream port:   Fa1/0/11 FEC Number:
  Hops from command device: 2
Device 'GenieTest' with member number 4
  Device type:      cisco SeaHorse
  MAC address:      0002.4b28.c480
  Upstream MAC address: 0030.946c.d740 (Cluster member 1)
  Local port:      Gi0/2   FEC number:
  Upstream port:   Fa0/9   FEC Number:
  Hops from command device: 2
Device 'Palpatine' with member number 5
  Device type:      cisco WS-C2924M-XL
  MAC address:      00b0.6404.f8c0
  Upstream MAC address: 0002.4b29.2e00 (Cluster member 0)
  Local port:      Gi2/1   FEC number:
  Upstream port:   Gi0/7   FEC Number:
  Hops from command device: 1
```

Related Commands

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

show controllers cpu-interface

Use the **show controllers cpu-interface** privileged EXEC command to display the state of the CPU network interface application-specific integrated circuit (ASIC) and the send and receive statistics for packets reaching the CPU.

show controllers cpu-interface [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines This display provides information that might be useful for Cisco technical support representatives troubleshooting the switch.

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

Examples This is a partial output example from the **show controllers cpu-interface** command:

```
Switch# show controllers cpu-interface
cpu-queue-frames  retrieved  dropped    invalid    hol-block
-----
rpc               4523063    0         0          0
stp              1545035    0         0          0
ipc              1903047    0         0          0
routing protocol  96145      0         0          0
L2 protocol      79596      0         0          0
remote console   0          0         0          0
sw forwarding    5756       0         0          0
host            225646     0         0          0
broadcast        46472      0         0          0
cbt-to-spt       0          0         0          0
igmp snooping    68411      0         0          0
icmp             0          0         0          0
logging          0          0         0          0
rpf-fail         0          0         0          0
queue14          0          0         0          0
cpu heartbeat    1710501    0         0          0
```

Supervisor ASIC receive-queue parameters

```
-----
queue 0 maxrecevsize 5EE pakhead 1419A20 paktail 13EAED4
```

show controllers cpu-interface

```
queue 1 maxrecevsize 5EE pakhead 15828E0 paktail 157FBFC
queue 2 maxrecevsize 5EE pakhead 1470D40 paktail 1470FE4
queue 3 maxrecevsize 5EE pakhead 19CDDDD0 paktail 19D02C8
```

<output truncated>

Supervisor ASIC Mic Registers

```
-----
MicDirectPollInfo          80000800
MicIndicationsReceived     00000000
MicInterruptsReceived      00000000
MicPcsInfo                 0001001F
MicPlbMasterConfiguration  00000000
MicRxFifosAvailable        00000000
MicRxFifosReady            0000BFFF
MicTimeOutPeriod:          FrameTOPeriod: 00000EA6 DirectTOPeriod: 00004000
```

<output truncated>

MicTransmitFifoInfo:

```
Fifo0:  StartPtrs:      038C2800      ReadPtr:      038C2C38
        WritePtrs:      038C2C38      Fifo_Flag:      8A800800
        Weights:        001E001E
Fifo1:  StartPtr:       03A9BC00      ReadPtr:       03A9BC60
        WritePtrs:      03A9BC60      Fifo_Flag:      89800400
        writeHeaderPtr: 03A9BC60
Fifo2:  StartPtr:       038C8800      ReadPtr:       038C88E0
        WritePtrs:      038C88E0      Fifo_Flag:      88800200
        writeHeaderPtr: 038C88E0
Fifo3:  StartPtr:       03C30400      ReadPtr:       03C30638
        WritePtrs:      03C30638      Fifo_Flag:      89800400
        writeHeaderPtr: 03C30638
Fifo4:  StartPtr:       03AD5000      ReadPtr:       03AD50A0
        WritePtrs:      03AD50A0      Fifo_Flag:      89800400
        writeHeaderPtr: 03AD50A0
Fifo5:  StartPtr:       03A7A600      ReadPtr:       03A7A600
        WritePtrs:      03A7A600      Fifo_Flag:      88800200
        writeHeaderPtr: 03A7A600
Fifo6:  StartPtr:       03BF8400      ReadPtr:       03BF87F0
        WritePtrs:      03BF87F0      Fifo_Flag:      89800400
```

<output truncated>

Related Commands

Command	Description
show controllers ethernet-controller	Displays per-interface send and receive statistics read from the hardware or the interface internal registers.
show interfaces	Displays the administrative and operational status of all interfaces or a specified interface.

show controllers ethernet-controller

Use the **show controllers ethernet-controller** privileged EXEC command without keywords to display per-port send and receive statistics read from the hardware. Use with the **phy** keyword to display the port internal registers or the **port-asic** keyword to display information about the port application-specific integrated circuit (ASIC).

show controllers ethernet-controller [[*interface-id*] [**phy** [**detail**] | **port-asic** {**configuration** | **statistics**}]] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

<i>interface-id</i>	The physical port (including type, module, and port number).
phy	(Optional) Display the status of the internal registers on the switch physical layer device (PHY) for the device or the port. This display includes the operational state of the automatic medium-dependent-interface crossover (Auto-MDIX) feature on a port.
detail	(Optional) Display details about the PHY internal registers.
port-asic	(Optional) Display information about the port ASIC internal registers.
configuration	Display port ASIC internal register configuration.
statistics	Display port ASIC statistics, including the Rx/Sup Queue and miscellaneous statistics.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC (supported with only the *interface-id* keywords in user EXEC mode)

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

This display without keywords provides traffic statistics, basically the Remote Network Monitoring (RMON) statistics for all ports or for the specified port.

When you enter the **phy** or **port-asic** keywords, the displayed information is useful primarily for Cisco technical support representatives troubleshooting the switch.

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

Examples

This is an example of output from the **show controllers ethernet-controller** command for a port:

Switch# **show controllers ethernet-controller gigabitethernet1/0/1**

Transmit GigabitEthernet1/0/1	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	

This is an example of output from the **show controllers ethernet-controller phy** command for a specific port. Note that the last line of the display shows the Auto-MDIX setting for the port.

Switch# **show controllers ethernet-controller fastethernet1/0/3 phy**

Control Register	:	0011 0001 0000 0000
Control STATUS	:	0111 1000 0000 1001
Phy ID 1	:	0000 0000 0001 0011
Phy ID 2	:	0111 1000 1111 1011
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 Rx Regi	:	0000 0000 0000 0000
Port Configuration Register	:	0000 0001 1010 0100
Port Status Register	:	0000 0001 0000 0000
Interrupt Enable Register	:	1010 0000 0000 0000
Interrupt Status Register	:	0000 0000 0101 0100
LED Configuration Register	:	1001 1001 1001 0000
Trim Enable Register	:	0000 1101 0000 0000
Auto-MDIX	:	Off [AdminState=0 Flags=0x00002248

This is an example of output from the **show controllers ethernet-controller port-asic configuration** command:

```
Switch# show controllers ethernet-controller port-asic configuration
=====
Switch 1, PortASIC 0 Registers
-----
DeviceType                : 000101BC
Reset                     : 00000000
PmadMicConfig             : 00000001
PmadMicDiag               : 00000003
SupervisorReceiveFifoSramInfo : 000007D0 000007D0 40000000
SupervisorTransmitFifoSramInfo : 000001D0 000001D0 40000000
GlobalStatus              : 00000800
IndicationStatus          : 00000000
IndicationStatusMask      : FFFFFFFF
InterruptStatus           : 00000000
InterruptStatusMask       : 01FFE800
SupervisorDiag            : 00000000
SupervisorFrameSizeLimit  : 000007C8
SupervisorBroadcast       : 000A0F01
GeneralIO                 : 000003F9 00000000 00000004
StackPcsInfo              : FFFF1000 860329BD 5555FFFF FFFFFFFF
                          FF0FFF00 86020000 5555FFFF 00000000
StackRacInfo              : 73001630 00000003 7F001644 00000003
                          24140003 FD632B00 18E418E0 FFFFFFFF
StackControlStatus        : 18E418E0
stackControlStatusMask    : FFFFFFFF
TransmitBufferFreeListInfo : 00000854 00000800 00000FF8 00000000
                          0000088A 0000085D 00000FF8 00000000
TransmitRingFifoInfo      : 00000016 00000016 40000000 00000000
                          0000000C 0000000C 40000000 00000000
TransmitBufferInfo        : 00012000 00000FFF 00000000 00000030
TransmitBufferCommonCount : 00000F7A
TransmitBufferCommonCountPeak : 0000001E
TransmitBufferCommonCommonEmpty : 000000FF
NetworkActivity           : 00000000 00000000 00000000 02400000
DroppedStatistics         : 00000000
FrameLengthDeltaSelect    : 00000001
SneakPortFifoInfo         : 00000000
MacInfo                   : 0EC0801C 00000001 0EC0801B 00000001
                          00C0001D 00000001 00C0001E 00000001
```

<output truncated>

This is an example of output from the **show controllers ethernet-controller port-asic statistics** command:

```
Switch# show controllers ethernet-controller port-asic statistics
=====
Switch 1, PortASIC 0 Statistics
-----
      0 RxQ-0, wt-0 enqueue frames      0 RxQ-0, wt-0 drop frames
4118966 RxQ-0, wt-1 enqueue frames      0 RxQ-0, wt-1 drop frames
      0 RxQ-0, wt-2 enqueue frames      0 RxQ-0, wt-2 drop frames

      0 RxQ-1, wt-0 enqueue frames      0 RxQ-1, wt-0 drop frames
    296 RxQ-1, wt-1 enqueue frames      0 RxQ-1, wt-1 drop frames
2836036 RxQ-1, wt-2 enqueue frames      0 RxQ-1, wt-2 drop frames

      0 RxQ-2, wt-0 enqueue frames      0 RxQ-2, wt-0 drop frames
      0 RxQ-2, wt-1 enqueue frames      0 RxQ-2, wt-1 drop frames
158377 RxQ-2, wt-2 enqueue frames      0 RxQ-2, wt-2 drop frames
```

show controllers ethernet-controller

```

0 RxQ-3, wt-0 enqueue frames
0 RxQ-3, wt-1 enqueue frames
0 RxQ-3, wt-2 enqueue frames

15 TxBufferFull Drop Count
0 TxBufferFrameDesc BadCrc16
0 TxBuffer Bandwidth Drop Cou
0 TxQueue Bandwidth Drop Coun
0 TxQueue Missed Drop Statist
74 RxBuffer Drop DestIndex Cou
0 SneakQueue Drop Count
0 Learning Queue Overflow Fra
0 Learning Cam Skip Count

15 Sup Queue 0 Drop Frames
0 Sup Queue 1 Drop Frames
0 Sup Queue 2 Drop Frames
0 Sup Queue 3 Drop Frames
0 Sup Queue 4 Drop Frames
0 Sup Queue 5 Drop Frames
0 Sup Queue 6 Drop Frames
0 Sup Queue 7 Drop Frames

0 RxQ-3, wt-0 drop frames
0 RxQ-3, wt-1 drop frames
0 RxQ-3, wt-2 drop frames

0 Rx Fcs Error Frames
0 Rx Invalid Oversize Frames
0 Rx Invalid Too Large Frames
0 Rx Invalid Too Large Frames
0 Rx Invalid Too Small Frames
0 Rx Too Old Frames
0 Tx Too Old Frames
0 System Fcs Error Frames

0 Sup Queue 8 Drop Frames
0 Sup Queue 9 Drop Frames
0 Sup Queue 10 Drop Frames
0 Sup Queue 11 Drop Frames
0 Sup Queue 12 Drop Frames
0 Sup Queue 13 Drop Frames
0 Sup Queue 14 Drop Frames
0 Sup Queue 15 Drop Frames
=====
Switch 1, PortASIC 1 Statistics
-----
0 RxQ-0, wt-0 enqueue frames
52 RxQ-0, wt-1 enqueue frames
0 RxQ-0, wt-2 enqueue frames

0 RxQ-0, wt-0 drop frames
0 RxQ-0, wt-1 drop frames
0 RxQ-0, wt-2 drop frames

<output truncated>

```

Related Commands

Command	Description
show boot	Displays the state of the CPU network ASIC and send and receive statistics for packets reaching the CPU.
show controllers tcam	Displays the state of registers for all ternary content addressable memory (TCAM) and TCAM ASICs.

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 port application-specific integrated circuits (ASICs) that are CAM controllers.

show controllers tcam [**asic** **number**]] [**detail**] [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description	
asic	(Optional) Display port ASIC TCAM information.
number	(Optional) Display information for the specified port ASIC number. The range is from 0 to 15.
detail	(Optional) Display detailed TCAM register information.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	This display provides information that might be useful for Cisco technical support representatives troubleshooting the switch. Expressions are case sensitive. For example, if you enter exclude output, the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

Examples	This is an example of output from the show controllers tcam command:

```
Switch# show controllers tcam
```

```
-----
TCAM-0 Registers
-----
```

```
REV:      00B30103
SIZE:     00080040
ID:       00000000
CCR:      00000000_F0000020

RPID0:    00000000_00000000
RPID1:    00000000_00000000
RPID2:    00000000_00000000
RPID3:    00000000_00000000

HRR0:     00000000_E000CAFC
HRR1:     00000000_00000000
```

show controllers tcam

```
HRR2:  00000000_00000000
HRR3:  00000000_00000000
HRR4:  00000000_00000000
HRR5:  00000000_00000000
HRR6:  00000000_00000000
HRR7:  00000000_00000000

<output truncated>

GMR31:  FF_FFFFFFFF_FFFFFFFF
GMR32:  FF_FFFFFFFF_FFFFFFFF
GMR33:  FF_FFFFFFFF_FFFFFFFF

=====
TCAM related PortASIC 1 registers
=====
LookupType:                89A1C67D_24E35F00
LastCamIndex:              0000FFE0
LocalNoMatch:              000069E0
ForwardingRamBaseAddress:
                            00022A00 0002FE00 00040600 0002FE00 0000D400
                            00000000 003FBA00 00009000 00009000 00040600
                            00000000 00012800 00012900
```

Related Commands

Command	Description
show controllers cpu-interface	Displays the state of the CPU network ASIC and send and receive statistics for packets reaching the CPU.
show controllers ethernet-controller	Displays per-port send and receive statistics read from the hardware or the port internal registers.

show cpu traffic qos

Use the **show cpu traffic qos** user EXEC command to display the Quality of Service (QoS) parameters for CPU-generated traffic.

show cpu traffic qos [**|** { **begin** | **exclude** | **include** } *expression*]

Syntax Description	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	User EXEC

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

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

Examples	This is an example of output from the show cpu traffic qos command:

```
Switch> show set cpu
QOS - CPU Generated Traffic
-----
Cos                2
DSCP               30
Precedence         3
```

Related Commands	Command	Description
	show mls qos	Displays the QoS configuration information.

show dot1q-tunnel

Use the **show dot1q-tunnel** user EXEC command to display information about 802.1Q tunnel ports.

show dot1q-tunnel [**interface** *interface-id*] [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description

interface <i>interface-id</i>	(Optional) Specify the interface for which to display 802.1Q tunneling information. Valid interfaces include physical ports and port channels.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show dot1q-tunnel** command:

```
Switch> show dot1q-tunnel
Port
-----
Gi1/1/1
Gi1/1/2
Po2
```

Related Commands

Command	Description
show vlan dot1q tag native	Displays 802.1Q native VLAN tagging status.
switchport mode dot1q-tunnel	Configures an interface as an 802.1Q tunnel port.

show dot1x

Use the **show dot1x** privileged EXEC command to display 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*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description	
all	(Optional) Display the 802.1x status for all ports.
interface <i>interface-id</i>	(Optional) Display the 802.1x status for the specified port (including type, module, and port number).
statistics interface <i>interface-id</i>	(Optional) Display 802.1x statistics for the switch or the specified port (including type, module, and port number).
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	If you do not specify a port, global parameters and a summary are displayed. If you specify a port, details for that port are displayed. Expressions are case sensitive. For example, if you enter exclude output, the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

Examples	This is an example of output from the show dot1x and the show dot1x all 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 FastEthernet1/0/3
-----
Supplicant MAC 00d0.b71b.35de
  AuthSM State      = CONNECTING
  BndSM 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 FastEthernet1/0/7

```

-----
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*** command:

Switch# **show dot1x interface fastethernet1/0/3**

```

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 2-19](#) describes the fields in the display.

Switch# **show dot1x statistics interface fastethernet1/0/3**

```

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 2-19 *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.

Table 2-19 *show dot1x statistics Field Descriptions (continued)*

Field	Description
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.
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 802.1x version 1 format.
LastRxSrcMac	Source MAC address carried in the most recently received EAPOL frame.

Related Commands

Command	Description
dot1x default	Resets the configurable 802.1x parameters to their default values.

show dtp

Use the **show dtp** privileged EXEC command to display Dynamic Trunking Protocol (DTP) information for the switch or for a specified interface.

```
show dtp [interface interface-id] [ | {begin | exclude | include} expression]
```

Syntax Description	interface interface-id	(Optional) Display port security settings for the specified interface. Valid interfaces include physical ports (including type, module, and port number).
	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	expression	Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

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

```
Switch# show dtp
Global DTP information
    Sending DTP Hello packets every 30 seconds
    Dynamic Trunk timeout is 300 seconds
    21 interfaces using DTP
```

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

```
Switch# show dtp interface fastethernet1/0/1
DTP information for FastEthernet1/0/1:
TOS/TAS/TNS:                ACCESS/AUTO/ACCESS
TOT/TAT/TNT:                NATIVE/NEGOTIATE/NATIVE
Neighbor address 1:         000943A7D081
Neighbor address 2:         000000000000
Hello timer expiration (sec/state): 1/RUNNING
Access timer expiration (sec/state): never/STOPPED
Negotiation timer expiration (sec/state): never/STOPPED
Multidrop timer expiration (sec/state): never/STOPPED
FSM state:                  S2:ACCESS
# times multi & trunk       0
Enabled:                    yes
In STP:                     no

Statistics
```

```

-----
3160 packets received (3160 good)
0 packets dropped
    0 nonegotiate, 0 bad version, 0 domain mismatches, 0 bad TLVs, 0 other
6320 packets output (6320 good)
    3160 native, 3160 software encap isl, 0 isl hardware native
0 output errors
0 trunk timeouts
1 link ups, last link up on Mon Mar 01 1993, 01:02:29
0 link downs

```

Related Commands

Command	Description
show interfaces trunk	Displays interface trunking information.

show env

Use the **show env** user EXEC command to display fan, temperature, redundant power system (RPS) availability, and power information for the switch.

```
show env {all | fan | power | rps| temperature} [ | {begin | exclude | include} expression]
```

Syntax Description	all	Display both fan and temperature environmental status.
	fan	Display the switch fan status.
	power	Display the switch power status.
	rps	Display whether an RPS 300 Redundant Power System is connected to the switch.
	temperature	Display the switch temperature status.
	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	expression	Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

Examples This is an example of output from the **show env all** command:

```
Switch> show env all
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
```

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

```
Switch> show env fan
FAN is OK
```

show errdisable detect

Use the **show errdisable detect** user EXEC command to display error-disabled detection status.

show errdisable detect [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.
	12.2(37)SE	The <i>Mode</i> column was added to the output display.

Usage Guidelines	The <i>Mode</i> 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 <i>gbic-invalid</i> error in the <i>Reason</i> column refers to an invalid small form-factor pluggable (SFP) interface.
Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.	

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
```

show errdisable detect

```

loopback          Enabled    port
lsgroup           Enabled    port
oam-remote-failur Enabled    port
pagp-flap         Enabled    port
psecure-violatio  Enabled    port/vlan
security-violatio Enabled    port
sfp-config-mismat Enabled    port
storm-control     Enabled    port
udld              Enabled    port
vmps              Enabled    port

```



Note

Though visible in the output, the dhcp-rate-limit and storm-control fields are not valid.

Related Commands

Command	Description
errdisable detect cause	Enables error-disabled detection for a specific cause or all causes.
show errdisable flap-values	Displays error condition recognition information.
show errdisable recovery	Displays error-disabled recovery timer information.
show interfaces status	Displays interface status or a list of interfaces in 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 [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.1(14)AX	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

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

Examples This is an example of output from the **show errdisable flap-values** command:

```
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
	errdisable detect cause	Enables error-disable detection for a specific cause or all causes.
	show errdisable detect	Displays error-disable detection status.
	show errdisable recovery	Displays error-disable recovery timer information.
	show interfaces status	Displays interface status or a list of interfaces in error-disabled state.

show errdisable recovery

Use the **show errdisable recovery** user EXEC command to display the error-disable recovery timer information.

show errdisable recovery [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.
	A gbic-invalid error-disable reason refers to an invalid small form-factor pluggable (SFP) interface.

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



Note

Though visible, the dhcp-rate-limit and unicast-flood reasons are not supported.

```
Switch> show errdisable recovery
ErrDisable Reason    Timer Status
-----
udld                  Disabled
bpduguard             Disabled
security-violatio    Disabled
channel-misconfig    Disabled
vmmps                 Disabled
pagp-flap             Disabled
dtp-flap              Disabled
link-flap             Disabled
gbic-invalid          Disabled
psecure-violation    Disabled
gbic-invalid          Disabled
dhcp-rate-limit       Disabled
unicast-flood         Disabled
loopback              Disabled

Timer interval:300 seconds

Interfaces that will be enabled at the next timeout:
```

show errdisable recovery

Interface	Errdisable reason	Time left(sec)
-----	-----	-----
Fa1/0/4	link-flap	279



Note

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

Related Commands

Command	Description
errdisable recovery	Configures the recover mechanism variables.
show errdisable detect	Displays error disable detection status.
show errdisable flap-values	Displays error condition recognition information.
show interfaces status	Displays interface status or a list of interfaces in error-disabled state.

show etherchannel

Use the **show etherchannel** user EXEC command to display EtherChannel information for a channel.

```
show etherchannel [channel-group-number {detail | port | port-channel | protocol | summary}]
                 {detail | load-balance | port | port-channel | protocol | summary} [ | {begin | exclude |
include} expression]
```

Syntax Description	
<i>channel-group-number</i>	(Optional) Number of the channel group. The range is 1 to 12.
detail	Display detailed EtherChannel information.
load-balance	Display the load-balance or frame-distribution scheme among interfaces in the port channel.
port	Display EtherChannel port information.
port-channel	Display port-channel information.
protocol	Display the protocol that is being used in the EtherChannel.
summary	Display a one-line summary per channel-group.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	If you do not specify a <i>channel-group</i>, all channel groups are displayed. In the output, the Passive port list field appears only for Layer 3 port channels. The appearance of 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). Expressions are case sensitive. For example, if you enter exclude output, the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

Examples	This is an example of output from the show etherchannel 1 detail command:

```
Switch> show etherchannel 1 detail
Group state = L2
Ports: 2    Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:   LACP
           Ports in the group:
           -----
Port: Gi1/0/1
```

show etherchannel

```

-----
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
Fa1/0/1   SA      bndl       32768       0x1     0x1    0x101  0x3D
Fa1/0/2   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     Gi1/0/1   Active        0
0       00     Gi1/0/2   Active        0

Time since last port bundled: 01d:20h:20m:20s  Gi1/0/2

```

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	Gi1/0/1 (P) Gi1/0/2 (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     Gi1/0/1   Active     0
  0      00     Gi1/0/2   Active     0

Time since last port bundled:    01d:20h:24m:44s    Gi1/0/2

```

This is an example of output from **show etherchannel protocol** command:

```

Switch# show etherchannel protocol
          Channel-group listing:
          -----
Group: 1
-----
Protocol: LACP

Group: 2
-----
Protocol: PAgP

```

Related Commands

Command	Description
channel-group	Assigns an Ethernet port to an EtherChannel group.
channel-protocol	Restricts the protocol used on an interface to manage channeling.
interface port-channel	Accesses or creates the port channel.

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**] [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description

id <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.
interface <i>interface-id</i>	(Optional) Display EVC information for the specified interface.
detail	(Optional) Display detailed information about EVC service or the specified EVC ID or interface.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)SEG	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show 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
ethernet evc <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**] [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description		
id <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.	
interface <i>interface-id</i>	(Optional) Display service-instance information for the specified interface.	
detail	(Optional) Display detailed information about service instances or the specified service-instance ID or interface.	
begin	(Optional) Display begins with the line that matches the <i>expression</i> .	
exclude	(Optional) Display excludes lines that match the <i>expression</i> .	
include	(Optional) Display includes lines that match the specified <i>expression</i> .	
<i>expression</i>	Expression in the output to use as a reference point.	

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.2(25)SEG	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

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
```

show ethernet service instance

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

Related Commands

Command	Description
service instance <i>id</i> ethernet	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**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description		
<i>interface-id</i>	(Optional) Display service-instance information for the specified interface.	
detail	(Optional) Display detailed information about service instances on all interfaces or the specified interface.	
begin	(Optional) Display begins with the line that matches the <i>expression</i> .	
exclude	(Optional) Display excludes lines that match the <i>expression</i> .	
include	(Optional) Display includes lines that match the specified <i>expression</i> .	
<i>expression</i>	Expression in the output to use as a reference point.	

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.2(25)SEG	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

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
```

show ethernet service interface

```
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
```

Related Commands

Command	Description
service instance <i>id</i> ethernet	Defines an Ethernet service instance and enters Ethernet service configuration mode from interface configuration mode.

show interfaces

Use the **show interfaces** privileged EXEC command to display the administrative and operational status of all interfaces or a specified interface.

```
show interfaces [interface-id | vlan vlan-id] [accounting | capabilities [module number] |
counters | description | etherchannel | flowcontrol | pruning | rep | stats | status
[err-disabled] | switchport [backup | module number] | [module number] | trunk] [ | {begin
| exclude | include} expression]
```

Syntax Description

interface-id	(Optional) Valid interfaces include physical ports (including type, module, and port number) and port channels. The port-channel range is 1 to 48.
vlan vlan-id	(Optional) VLAN identification. The range is 1 to 4094.
accounting	(Optional) Display accounting information on the interface, including active protocols and input and output packets and octets.
	Note The display shows only packets processed in software; hardware-switched packets do not appear.
capabilities	(Optional) Display the capabilities of all interfaces or the specified interface, including the features and options that you can configure on the interface. Though visible in the command line help, this option is not available for VLAN IDs.
module number	(Optional) Display capabilities or switchport configuration characteristics (depending on preceding keyword) of all interfaces on the switch. The range is 1 to 9. This option is not available if you entered a specific interface ID.
counters	(Optional) See the show interfaces counters command.
description	(Optional) Display the administrative status and description set for an interface.
etherchannel	(Optional) Display interface EtherChannel information.
flowcontrol	(Optional) Display interface flowcontrol information
pruning	(Optional) Display interface trunk VTP pruning information.
rep	(Optional) See the show interfaces rep command.
stats	(Optional) Display the input and output packets by switching path for the interface.
status	(Optional) Display the status of the interface. A status of <i>unsupported</i> in the Type field means that a non-Cisco small form-factor pluggable (SFP) module is inserted in the module slot.
err-disabled	(Optional) Display interfaces in error-disabled state.
switchport	(Optional) Display the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
backup	(Optional) Display Flex Link backup interface configuration and status for the specified interface.
trunk	Display interface trunk information. If you do not specify an interface, only information for active trunking ports appears.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .

l include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

**Note**

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.
12.2(25)EY	The backup , properties , and private-vlan mapping keywords were added.
12.2(25)SEE	Added the backup , counters , detail , and trunk keywords.

Usage Guidelines

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

- Entering **show interface capabilities module 1** displays the capabilities of all interfaces on the switch. If you enter a number other than 1, the output is blank. This keyword is not available if you enter a specific interface ID before the **capabilities** keyword.
- Entering **show interfaces interface-id capabilities** displays the capabilities of the specified interface.
- Entering **show interfaces capabilities** (with no module number or interface ID) displays the capabilities of all interfaces on the switch.

The **vlan mapping** option is available only when you have entered any *interface-ID* or **vlan vlan-id**; however, the display shows VLAN mapping information only for ES ports.

Expressions are case sensitive. For example, if you enter **l exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

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

```
Switch# show interfaces gigabitethernet0/2
GigabitEthernet0/2 is up, line protocol is up (connected) (vlan-err-dis)
  Hardware is Gigabit Ethernet, address is 0018.1902.cd02 (bia 0018.1902.cd02)
  MTU 1548 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive not set
Full-duplex, 1000Mb/s, link type is auto, media type is 10/100/1000BaseTX
input flow-control is off, output flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, 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
 12112813 packets input, 801716512 bytes, 0 no buffer
Received 2001806 broadcasts (0 multicasts)
 0 runs, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
 0 watchdog, 2001806 multicast, 0 pause input
 0 input packets with dribble condition detected
11935759 packets output, 783067011 bytes, 0 underruns
 0 output errors, 0 collisions, 2 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.

GigabitEthernet1/0/1
      Protocol    Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.
GigabitEthernet1/0/2
      Protocol    Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.

<output truncated>

```

This is an example of output from the **show interfaces capabilities** command for an interface.

```

Switch# show interfaces gigabitethernet1/0/2 capabilities
GigabitEthernet1/0/2
Model:                WS-C3750G-24TS
Type:                 10/100/1000BaseTX
Speed:                10,100,1000,auto
Duplex:               full,auto
Trunk encap. type:    802.1Q,ISL
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
Inline power:         no
SPAN:                 source/destination
PortSecure:           yes
Dot1x:                yes

```

This is an example of output from the **show interfaces interface description** command when the interface has been described as *Connects to Marketing* by using the **description** interface configuration command.

```
Switch# show interfaces gigabitethernet1/0/2 description
Interface Status      Protocol Description
Gi1/0/2      up          down      Connects to Marketing
```

This is an example of output from the **show interfaces etherchannel** command when port channels are configured on the switch:

```
Switch# show interfaces etherchannel
----
Port-channel1:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port        = 10/1          Number of ports = 0
GC                        = 0x00000000    HotStandBy port = null
Port state                = Port-channel Ag-Not-Inuse

Port-channel2:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port        = 10/2          Number of ports = 0
GC                        = 0x00000000    HotStandBy port = null
Port state                = Port-channel Ag-Not-Inuse

Port-channel3:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port        = 10/3          Number of ports = 0
GC                        = 0x00000000    HotStandBy port = null
Port state                = Port-channel Ag-Not-Inuse
```

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

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

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

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

```
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
Fa1/0/1                    connected   routed    a-half  a-100  10/100BaseTX
Fa1/0/2                    notconnect  121,40    auto    auto   10/100BaseTX
Fa1/0/3                    notconnect  1         auto    auto   10/100BaseTX
Fa1/0/4                    notconnect  18        auto    auto   Not Present
Fa1/0/5                    connected   121       a-full  a-1000 10/100BaseTX
Fa1/0/6                    connected   122,11    a-full  a-1000 10/100BaseTX

<output truncated>
Gi1/0/1                    notconnect  1         auto    auto   10/100/1000BaseTX
Gi1/0/2                    connected   vl-err-dis a-full  a-1000 10/100/1000BaseTX
```


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

```
Switch# show interfaces gigabitethernet1/0/2 status err-disabled
```

Port	Name	Status	Reason	Err-disabled Vlans
Gil/0/2		connected	elmi evc down	1,200

This is an example of output from the **show interfaces switchport** command for a port. [Table 2-20](#) 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 gigabitethernet1/0/1 switchport
```

```
Name: Gi1/0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled

Voice VLAN: none (Inactive)
Appliance trust: none
```

Table 2-20 *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.
Operational Trunking Encapsulation	
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. Lists the allowed VLANs on the trunk. Lists the active VLANs on the trunk.
Trunking VLANs Enabled	
Trunking VLANs Active	

Table 2-20 *show interfaces switchport Field Descriptions (continued)*

Field	Description
Pruning VLANs Enabled	Lists the VLANs that are pruning-eligible.
Protected	Displays whether or not protected port is enabled (True) or disabled (False) on the interface.
Unknown unicast blocked Unknown multicast blocked	Displays whether or not unknown multicast and unknown unicast traffic is blocked on the interface.
Voice VLAN	Displays the VLAN ID on which voice VLAN is enabled.
Appliance trust	Displays the class of service (CoS) setting of the data packets of the IP phone.

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

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
      Active Interface      Backup Interface      State
-----
Fa1/0/1                    Fa1/0/2              Active Up/Backup Standby
Fa3/0/3                    Fa4/0/5              Active Down/Backup Up
Po1                        Po2                  Active Standby/Backup Up
```

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

```
Switch# show interfaces gigabitEthernet1/0/2 pruning
Port      Vlans pruned for lack of request by neighbor
```

This is an example of output from the **show interfaces 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
-----
GigabitEthernet0/6    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, Gi0/8 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    GigabitEthernet0/8    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
GigabitEthernet0/6	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 gigabitethernet1/0/1 trunk
Port      Mode      Encapsulation  Status      Native vlan
Gi1/0/1   auto      negotiate      trunking    1

Port      Vlans allowed on trunk
Gi1/0/1   1-4094

Port      Vlans allowed and active in management domain
Gi1/0/1   1-4

Port      Vlans in spanning tree forwarding state and not pruned
Gi1/0/1   1-4
```

Related Commands

Command	Description
switchport access	Configures a port as a static-access or a dynamic-access port.
switchport block	Blocks unknown unicast or multicast traffic on an interface.
switchport backup interface	Configures Flex Links, a pair of Layer 2 interfaces that provide mutual backup.
switchport mode	Configures the VLAN membership mode of a port.

Command	Description
switchport protected	Isolates unicast, multicast, and broadcast traffic at Layer 2 from other protected ports on the same switch.
switchport trunk pruning	Configures the VLAN pruning-eligible list for ports in trunking mode.

show interfaces counters

Use the **show interfaces counters** privileged EXEC command to display various counters for the switch or for a specific interface.

show interfaces [*interface-id* | **vlan** *vlan-id*] **counters** [**errors** | **etherchannel** | **module** *switch-number* | **protocol status** | **trunk**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description		
<i>interface-id</i>	(Optional) ID of the physical interface, including type, module, and port number.	
errors	(Optional) Display error counters.	
etherchannel	(Optional) Display EtherChannel counters, including octets, broadcast packets, multicast packets, and unicast packets received and sent.	
module <i>switch-number</i>	(Optional) Display counters for the specified module. The only valid value is 1.	
protocol status	(Optional) Display status of protocols enabled on interfaces.	
trunk	(Optional) Display trunk counters.	
begin	(Optional) Display begins with the line that matches the <i>expression</i> .	
exclude	(Optional) Display excludes lines that match the <i>expression</i> .	
include	(Optional) Display includes lines that match the specified <i>expression</i> .	
<i>expression</i>	Expression in the output to use as a reference point.	



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
	12.1(14)AX	This command was introduced.
	12.2(25)EY	The etherchannel and protocol status keywords were added. The broadcast , multicast , and unicast keywords were removed.

Usage Guidelines	If you do not enter any keywords, all counters for all interfaces are included. Expressions are case sensitive. For example, if you enter exclude output, the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

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

```
Switch# show interfaces counters
Port          InOctets    InUcastPkts  InMcastPkts  InBcastPkts
```

show interfaces counters

```

Gi1/0/1          0          0          0          0
Gi1/0/2          0          0          0          0

```

<output truncated>

This is an example of partial output from the **show interfaces counters module** command.

```

Switch# show interfaces counters module 1
Port          InOctets    InUcastPkts  InMcastPkts  InBcastPkts
Fa1/0/1       475256      105          4335         593
Fa1/0/2       0           0            0            0
Fa1/0/3       0           0            0            0
Fa1/0/4       0           0            0            0
Fa1/0/5       0           0            0            0
Fa1/0/6       0           0            0            0
Fa1/0/7       0           0            0            0
Fa1/0/8       0           0            0            0
Fa1/0/9       0           0            0            0
Fa1/0/10      0           0            0            0
Fa1/0/11      0           0            0            0
Fa1/0/12      0           0            0            0
Fa1/0/13      5689160    11548        63746        0
Fa1/0/14      1998856    11547        6092         0
Fa1/0/15      1999304    11548        6095         0
Fa1/0/16      1999752    11547        6099         0
Fa1/0/17      1999496    11547        6097         0

```

<output truncated>

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

```

Switch# show interfaces counters protocol status
Protocols allocated:
Vlan1: Other, IP
Vlan20: Other, IP, ARP
Vlan30: Other, IP, ARP
Vlan40: Other, IP, ARP
Vlan50: Other, IP, ARP
Vlan60: Other, IP, ARP
Vlan70: Other, IP, ARP
Vlan80: Other, IP, ARP
Vlan90: Other, IP, ARP
Vlan900: Other, IP, ARP
Vlan3000: Other, IP
Vlan3500: Other, IP
FastEthernet1/0/1: Other, IP, ARP, CDP
FastEthernet1/0/2: Other, IP
FastEthernet1/0/3: Other, IP
FastEthernet1/0/4: Other, IP
FastEthernet1/0/5: Other, IP
FastEthernet1/0/6: Other, IP
FastEthernet1/0/7: Other, IP
FastEthernet1/0/8: Other, IP
FastEthernet1/0/9: Other, IP
FastEthernet1/0/10: Other, IP, CDP

```

<output truncated>

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

```

Switch# show interfaces counters trunk
Port          TrunkFramesTx  TrunkFramesRx  WrongEncap
Fa1/0/1       0              0              0

```

```

Fa1/0/2          0          0          0
Fa1/0/3        80678        4155        0
Fa1/0/4        82320        126         0
Fa1/0/5          0          0          0

```

<output truncated>

Related Commands

Command	Description
show interfaces	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**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

<i>interface-id</i>	(Optional) Display REP configuration and status for a specified physical interface or port channel ID.
detail	(Optional) Display detailed REP configuration and status information.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)SE	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.

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

Examples

This is sample output from the **show interface rep** command:

```
Switch # show interface rep
Interface          Seg-id   Type      LinkOp    Role
-----
GigabitEthernet1/0/1    1      Primary Edge   TWO_WAY   Open
GigabitEthernet1/0/2    1      Edge      TWO_WAY   Open
FastEthernet1/0/4       2              INIT_DOWN Fail
```


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
-----
GigabitEthernet1/0/1      1              NO_NEIGHBOR FailNoNbr
GigabitEthernet1/0/2      2              NO_NEIGHBOR FailLogOpen
```

This is sample output from the **show interface rep detail** command for a specified interface:

```
Switch # show interface gigabitethernet1/0/2 rep detail
GigabitEthernet1/0/2  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
rep segment	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 rep topology [detail]	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** | **dom-supported-list** | **module** *number* | **properties** | **threshold-table**] [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description

<i>interface-id</i>	(Optional) Display configuration and status for a specified physical interface.
detail	(Optional) Display calibration properties, including high and low numbers and any alarm information for any Digital Optical Monitoring (DoM)-capable transceiver if one is installed in the switch.
dom-supported-list	(Optional) List all supported DoM transceivers.
<i>module number</i>	(Optional) Limit display to interfaces on module on the switch. The range is 1 to 9. This option is not available if you entered a specific interface ID.
properties	(Optional) Display speed, duplex, and inline power settings on an interface.
threshold-table	(Optional) Display alarm and warning threshold table
 begin	(Optional) Display begins with the line that matches the <i>expression</i>
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(25)EY	This command was introduced.
12.2(44)SE	The dom-supported-list and threshold-table keywords were added.

Usage Guidelines

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

Examples

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

```
Switch# show interfaces gigabitethernet1/0/1 transceiver properties
Name : Gi1/0/1
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 gigabitethernet1/0/3 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)
Gi1/0/3	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)
Gi1/0/3	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)
Gi1/0/3	31.0	84.0	70.0	4.0	2.0

Port	Optical Transmit Power (dBm)	High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi1/0/3	-0.0 (-0.0)	-0.0	-0.0	-0.0	-0.0

Port	Optical Receive Power (dBm)	High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi1/0/3	N/A (-0.0) --	-0.0	-0.0	-0.0	-0.0

This is an example of output from the **show interfaces transceiver dom-supported-list** command:

```
Switch# show interfaces transceiver dom-supported-list
Transceiver Type          Cisco p/n min version
                          supporting DOM
-----
DWDm GBIC                 ALL
DWDm SFP                  ALL
RX only WDM GBIC          ALL
DWDm XENPAK                ALL
DWDm X2                    ALL
DWDm XFP                   ALL
CWDm GBIC                  NONE
CWDm X2                    ALL
CWDm XFP                   ALL
XENPAK ZR                  ALL
X2 ZR                      ALL
XFP ZR                     ALL
Rx_only_WDM_XENPAK        ALL
XENPAK_ER                  10-1888-03
X2_ER                      ALL
XFP_ER                     ALL
XENPAK_LR                  10-1838-04
```

show interfaces transceivers

```
X2_LR
ALL
<output truncated>
```

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

Optical Tx	Optical Rx	Temp	Laser Bias	Voltage current	
-----	-----	-----	-----	-----	-----
DWDM GBIC					
Min1	-0.50	-28.50	0	N/A	4.50
Min2	-0.30	-28.29	5	N/A	4.75
Max2	3.29	-6.69	60	N/A	5.25
Max1	3.50	6.00	70	N/A	5.50
DWDM SFP					
Min1	-0.50	-28.50	0	N/A	3.00
Min2	-0.30	-28.29	5	N/A	3.09
Max2	4.30	-9.50	60	N/A	3.59
Max1	4.50	9.30	70	N/A	3.70
RX only WDM GBIC					
Min1	N/A	-28.50	0	N/A	4.50
Min2	N/A	-28.29	5	N/A	4.75
Max2	N/A	-6.69	60	N/A	5.25
Max1	N/A	6.00	70	N/A	5.50
DWDM XENPAK					
Min1	-1.50	-24.50	0	N/A	N/A
Min2	-1.29	-24.29	5	N/A	N/A
Max2	3.29	-6.69	60	N/A	N/A
Max1	3.50	4.00	70	N/A	N/A
DWDM X2					
Min1	-1.50	-24.50	0	N/A	N/A
Min2	-1.29	-24.29	5	N/A	N/A
Max2	3.29	-6.69	60	N/A	N/A
Max1	3.50	4.00	70	N/A	N/A
DWDM XFP					
Min1	-1.50	-24.50	0	N/A	N/A
Min2	-1.29	-24.29	5	N/A	N/A
Max2	3.29	-6.69	60	N/A	N/A
Max1	3.50	4.00	70	N/A	N/A
CWDM X2					
Min1	N/A	N/A	0	N/A	N/A
Min2	N/A	N/A	0	N/A	N/A
Max2	N/A	N/A	0	N/A	N/A
Max1	N/A	N/A	0	N/A	N/A

Related Commands

Command	Description
show interfaces	Displays additional interface characteristics.

show inventory

Use the **show inventory** user EXEC command to display product identification (PID) information for the hardware.

show inventory [*entity-name* | **raw**] [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description

<i>entity-name</i>	(Optional) Display the specified entity. For example, enter the interface (such as gigabitethernet0/1) into which a small form-factor pluggable (SFP) module is installed.
raw	(Optional) Display every entity in the device.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(25)SEG	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 compact 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.

If there is no PID, no output appears when you enter the **show inventory** command.

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

Examples

This is example output from the **show inventory** command:

```
Switch> show inventory
NAME: "1", DESCR: "ME-C3750-24TE"
PID:                , VID:                , SN:

NAME: "GigabitEthernet1/1/2", DESCR: "1000BaseSX SFP"
PID:                , VID:                , SN: A50015093
```

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*] [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description		
interfaces <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.	
log	(Optional) Display the configuration and contents of the dynamic ARP inspection log buffer.	
statistics [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.	
vlan <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.	
begin	(Optional) Display begins with the line that matches the <i>expression</i> .	
exclude	(Optional) Display excludes lines that match the <i>expression</i> .	
include	(Optional) Display includes lines that match the specified <i>expression</i> .	
<i>expression</i>	Expression in the output to use as a reference point.	

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(25)EY	This command was introduced.
	12.2(37)SE	The output changed to include Probe Logging information.

Usage Guidelines Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show 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
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
Gi1/0/1	Untrusted	15	1
Gi1/0/2	Untrusted	15	1
Gi1/0/3	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 gigabitethernet1/0/1
```

Interface	Trust State	Rate (pps)	Burst Interval
Gi1/0/1	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
Gi1/0/1	5	0003.0000.d673	192.2.10.4	5	DHCP Deny	19:39:01 UTC
Mon Mar 1 1993						
Gi1/0/1	5	0001.0000.d774	128.1.9.25	6	DHCP Deny	19:39:02 UTC
Mon Mar 1 1993						
Gi1/0/1	5	0001.c940.1111	10.10.10.1	7	DHCP Deny	19:39:03 UTC
Mon Mar 1 1993						
Gi1/0/1	5	0001.c940.1112	10.10.10.2	8	DHCP Deny	19:39:04 UTC
Mon Mar 1 1993						
Gi1/0/1	5	0001.c940.1114	173.1.1.1	10	DHCP Deny	19:39:06 UTC
Mon Mar 1 1993						

show ip arp inspection

```

Gi1/0/1      5      0001.c940.1115  173.1.1.2      11  DHCP Deny      19:39:07 UTC
Mon Mar 1 1993
Gi1/0/1      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

```

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
arp access-list	Defines an ARP ACL.
clear ip arp inspection log	Clears the dynamic ARP inspection log buffer.
clear ip arp inspection statistics	Clears the dynamic ARP inspection statistics.
ip arp inspection log-buffer	Configures the dynamic ARP inspection logging buffer.
ip arp inspection vlan logging	Controls the type of packets that are logged per VLAN.
show arp access-list	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(25)EY	This command was introduced.
	12.2(25)SEE	The command output was updated to show the global suboption configuration.

Usage Guidelines Expressions are case sensitive. For example, if you enter **exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

This command displays only the results of global configuration. Therefore, in this example, the circuit ID suboption appears in its default format of **vlan-mod-port**, even if a string is configured for the circuit ID.

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
    circuit-id format: vlan-mod-port
    remote-id format: string
Verification of hwaddr field is enabled
Interface                Trusted      Rate limit (pps)
-----
FastEthernet1/0/1        yes         unlimited
FastEthernet1/0/2        yes         unlimited
FastEthernet1/0/3        no          2000
FastEthernet1/0/4        yes         unlimited
```

Related Commands	Command	Description
	show ip dhcp snooping binding	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*]
[| {**begin** | **exclude** | **include**} *expression*]

Syntax Description	<i>ip-address</i>	(Optional) Specify the binding entry IP address.
	<i>mac-address</i>	(Optional) Specify the binding entry MAC address.
	interface <i>interface-id</i>	(Optional) Specify the binding input interface.
	vlan <i>vlan-id</i>	(Optional) Specify the binding entry VLAN.
	begin	Display begins with the line that matches the <i>expression</i> .
	exclude	Display excludes lines that match the <i>expression</i> .
	include	Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.2(25)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.

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples This example shows how to display the 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    GigabitEthernet1/0/1
00:D0:B7:1B:35:DE   10.1.2.151         237         dhcp-snooping    20    GigabitEthernet1/0/2
Total number of bindings: 2
```

show ip dhcp snooping binding

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    GigabitEthernet1/0/1
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    GigabitEthernet1/0/2
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 gigabitethernet1/0/2
-----
MacAddress      IpAddress      Lease(sec)  Type           VLAN  Interface
-----
00:30:94:C2:EF:35  10.1.2.151    290         dhcp-snooping  20    GigabitEthernet1/0/2
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    GigabitEthernet1/0/1
00:00:00:00:00:02  10.1.2.151    65          dhcp-snooping  20    GigabitEthernet1/0/2
Total number of bindings: 2
```

Table 2-21 describes the fields in the **show ip dhcp snooping binding** command output:

Table 2-21 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
	Note 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
ip dhcp snooping binding	Configures the DHCP snooping binding database
show ip dhcp snooping	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**] [**| {begin | exclude | include} expression**]

Syntax Description	detail	(Optional) Display detailed status and statistics information.
	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	expression	Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.2(25)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 Succeed 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 Succeed Time : None
```

■ show ip dhcp snooping database

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
ip dhcp snooping	Enables DHCP snooping on a VLAN.
ip dhcp snooping database	Configures the DHCP snooping binding database agent or the binding file.
show ip dhcp snooping	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**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description	detail	(Optional) Display detailed statistics information.
	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.2(37)SE	This command was introduced.

Usage Guidelines Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

In a switch stack, all statistics are generated on the stack master. If a new stack master is elected, the statistics counters reset.

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 2-22 shows the DHCP snooping statistics and their descriptions:

Table 2-22 DHCP Snooping Statistics

DHCP Snooping Statistic	Description
Packets Processed by DHCP Snooping	Total number of packets handled by DHCP snooping, including forwarded and dropped packets.
Packets Dropped Because IDB not known	Number of errors when the input interface of the packet cannot be determined.
Queue full	Number of errors when an internal queue used to process the packets is full. This might happen if DHCP packets are received at an excessively high rate and rate limiting is not enabled on the ingress ports.
Interface is in errdisabled	Number of times a packet was received on a port that has been marked as error disabled. This might happen if packets are in the processing queue when a port is put into the error-disabled state and those packets are subsequently processed.
Rate limit exceeded	Number of times the rate limit configured on the port was exceeded and the interface was put into the error-disabled state.
Received on untrusted ports	Number of times a DHCP server packet (OFFER, ACK, NAK, or LEASEQUERY) was received on an untrusted port and was dropped.
Nonzero giaddr	Number of times the relay agent address field (giaddr) in the DHCP packet received on an untrusted port was not zero, or the no ip dhcp snooping information option allow-untrusted global configuration command is not configured and a packet received on an untrusted port contained option-82 data.
Source mac not equal to chaddr	Number of times the client MAC address field of the DHCP packet (chaddr) does not match the packet source MAC address and the ip dhcp snooping verify mac-address global configuration command is configured.
Binding mismatch	Number of times a RELEASE or DECLINE packet was received on a port that is different than the port in the binding for that MAC address-VLAN pair. This indicates someone might be trying to spoof the real client, or it could mean that the client has moved to another port on the switch and issued a RELEASE or DECLINE. The MAC address is taken from the chaddr field of the DHCP packet, not the source MAC address in the Ethernet header.

Table 2-22 DHCP Snooping Statistics (continued)

DHCP Snooping Statistic	Description
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.
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 IPSPG 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
clear ip dhcp snooping	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 view all configured Internet Group Management Protocol (IGMP) profiles or a specified IGMP profile.

show ip igmp profile [*profile number*] [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description

<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.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

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

Examples

These are examples of output from the **show ip igmp profile** command, with and without specifying a profile number. If no profile number is entered, the display includes all profiles configured on the switch.

```
Switch# show ip igmp profile 40
IGMP Profile 40
  permit
  range 233.1.1.1 233.255.255.255
```

```
Switch# show ip igmp profile
IGMP Profile 3
  range 230.9.9.0 230.9.9.0
IGMP Profile 4
  permit
  range 229.9.9.0 229.255.255.255
```

Related Commands

Command	Description
ip igmp profile	Configures the specified IGMP profile number.

show ip igmp snooping

Use the **show ip igmp snooping** privileged 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*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description	groups	(Optional) See the show ip igmp snooping groups command.
	mrouter	(Optional) See the show ip igmp snooping mrouter command.
	querier	(Optional) See the show ip igmp snooping querier command.
	vlan <i>vlan-id</i>	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.
	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.
	12.2(25)EY	The groups keyword was added. The show ip igmp snooping groups command replaced the show ip igmp snooping multicast command.

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 for IGMP snooping.

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

Examples This is an example of output from the **show ip igmp snooping** command. It shows how to display snooping characteristics for all VLANs on the switch.

```
Switch# show ip igmp snooping
vlan 1
-----
IGMP snooping is globally enabled
IGMP snooping TCN solicit query is globally disabled
IGMP snooping global TCN flood query count is 2
IGMP snooping is enabled on this Vlan
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
IGMP snooping source only learning age timer is 10
IGMP snooping is running in IGMP_ONLY mode on this Vlan
```

■ show ip igmp snooping

```
IGMP snooping report suppression is enabled on this Vlan
vlan 2
-----
```

```
IGMP snooping is globally enabled
IGMP snooping TCN solicit query is globally disabled
IGMP snooping global TCN flood query count is 2
```

<output truncated>

This is an example of output from the **show ip igmp snooping vlan 1** command. It shows how to display snooping characteristics for a specific VLAN.

```
Switch# show ip igmp snooping vlan 1
vlan 1
-----
IGMP snooping is globally enabled
IGMP snooping TCN solicit query is globally disabled
IGMP snooping global TCN flood query count is 2
IGMP snooping is enabled on this Vlan
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
IGMP snooping source only learning age timer is 10
IGMP snooping is running in IGMP_ONLY mode on this Vlan
IGMP snooping report suppression is enabled on this Vlan
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
ip igmp snooping querier	Enables the IGMP querier function in Layer 2 networks.
ip igmp snooping report-suppression	Enables IGMP report suppression.
ip igmp snooping vlan immediate-leave	Enables IGMP snooping immediate-leave processing on a VLAN.
ip igmp snooping vlan mrouter	Adds a multicast router port or configures the multicast learning method.
ip igmp snooping vlan static	Statically adds a Layer 2 port as a member of a multicast group.
show ip igmp snooping groups	Displays the IGMP snooping multicast table for the switch.
show ip igmp snooping mrouter	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN.
show ip igmp snooping querier	Displays the configuration and operation information for the IGMP querier configured on a switch.

show ip igmp snooping groups

Use the **show ip igmp snooping groups** privileged EXEC command to display the Internet Group Management Protocol (IGMP) snooping multicast table for the switch or the multicast information. Use with the **vlan** keyword to display the multicast table for a specified multicast VLAN or specific multicast information.

show ip igmp snooping groups [**count** | **dynamic** [**count**] | **user** [**count**]] [| {**begin** | **exclude** | **include**} *expression*]

show ip igmp snooping groups vlan *vlan-id* [*ip_address* | **count** | **dynamic** [**count**] | **user** [**count**]] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description	
count	(Optional) Display the total number of entries for the specified command options instead of the actual entries.
dynamic	(Optional) Display entries learned by IGMP snooping.
user	(Optional) Display only the user-configured multicast entries.
<i>ip_address</i>	(Optional) Display characteristics of the multicast group with the specified group IP address.
vlan <i>vlan-id</i>	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(25)EY	This command was introduced. It replaced the show ip igmp snooping multicast command.

Usage Guidelines

Use this command to display multicast information or the multicast table.

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

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show ip igmp snooping groups** command without any keywords. It displays the multicast table for the switch.

```
Switch# show ip igmp snooping groups
```

Vlan	Group	Type	Version	Port List
1	224.1.4.4	igmp		Fa1/0/11
1	224.1.4.5	igmp		Fa1/0/11
2	224.0.1.40	igmp	v2	Fa1/0/15

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	Gi2/0/1, Fa1/0/15
104	224.1.4.3	igmp	v2	Gi2/0/1, Fa1/0/15

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	Gi2/0/1, Fa1/0/15

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
ip igmp snooping vlan mrouter	Configures a multicast router port.
ip igmp snooping vlan static	Statically adds a Layer 2 port as a member of a multicast group.
show ip igmp snooping	Displays the IGMP snooping configuration of the switch or the VLAN.
show ip igmp snooping mrouter	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN.

show ip igmp snooping mrouter

Use the **show ip igmp snooping mrouter** privileged EXEC command to display the Internet Group Management Protocol (IGMP) snooping dynamically learned and manually configured multicast router ports for the switch or for the specified multicast VLAN.

show ip igmp snooping mrouter [**vlan** *vlan-id*] [**|** { **begin** | **exclude** | **include** } *expression*]

Syntax Description	vlan <i>vlan-id</i>	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.
	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	Use this command to display multicast router ports on the switch or for a specific VLAN.
	VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.
	When multicast VLAN registration (MVR) is enabled, the show ip igmp snooping mrouter command displays MVR multicast router information and IGMP snooping information.
	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

Examples	This is an example of output from the show ip igmp snooping mrouter command. It shows how to display multicast router ports on the switch.

```
Switch# show ip igmp snooping mrouter
Vlan      ports
----      -
200       Fa1/0/13(static), Fa1/0/14(static)
```

Related Commands	Command	Description
	ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
	ip igmp snooping vlan mrouter	Adds a multicast router port.
	ip igmp snooping vlan static	Statically adds a Layer 2 port as a member of a multicast group.

Command	Description
show ip igmp snooping	Displays the IGMP snooping configuration of the switch or the VLAN
show ip igmp snooping groups	Displays IGMP snooping multicast information for the switch or for the specified parameter.

show ip igmp snooping querier

Use the **show ip igmp snooping querier detail** user EXEC command to display the configuration and operation information for the IGMP querier configured on a switch.

show ip igmp snooping querier [**detail** | **vlan** *vlan-id* [**detail**]] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description		
detail		Optional) Display detailed IGMP querier information.
vlan <i>vlan-id</i> [detail]		Optional) Display IGMP querier information for the specified VLAN. The range is 1 to 1001 and 1006 to 4094. Use the detail keyword to display detailed information.
begin		(Optional) Display begins with the line that matches the <i>expression</i> .
exclude		(Optional) Display excludes lines that match the <i>expression</i> .
include		(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>		Expression in the output to use as a reference point.

Command Modes User EXEC

Command History	Release	Modification
	12.2(25)EY	This command was introduced.

Usage Guidelines Use the **show ip igmp snooping querier** command to display the IGMP version and the IP address of a detected device, also called a *querier*, that sends IGMP query messages. A subnet can have multiple multicast routers but has only one IGMP querier. In a subnet running IGMPv2, one of the multicast routers is elected as the querier. The querier can be a Layer 3 switch.

The **show ip igmp snooping querier** command output also shows the VLAN and the interface on which the querier was detected. If the querier is the switch, the output shows the *Port* field as *Router*. If the querier is a router, the output shows the port number on which the querier is learned in the *Port* field.

The **show ip igmp snooping querier detail** user EXEC command is similar to the **show ip igmp snooping querier** command. However, the **show ip igmp snooping querier** command displays only the device IP address most recently detected by the switch querier.

The **show ip igmp snooping querier detail** command displays the device IP address most recently detected by the switch querier 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

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show ip igmp snooping querier** command:

```
Switch> show ip igmp snooping querier
Vlan      IP Address      IGMP Version      Port
-----
1         172.20.50.11    v3                 Gi1/0/1
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                 Fa1/0/1

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 Fa1/0/1
-----
admin state           : Enabled
admin version         : 2
source IP address     : 10.1.1.65
query-interval (sec)  : 60
max-response-time (sec) : 10
querier-timeout (sec) : 120
tcn query count       : 2
tcn query interval (sec) : 10
operational state     : Non-Querier
operational version   : 2
tcn query pending count : 0
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
ip igmp snooping querier	Enables the IGMP querier function in Layer 2 networks.
show ip igmp snooping	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN.

show 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**] [**interface** *interface-id*] [**vlan** *vlan-id*] [| { **begin** | **exclude** | **include** } *expression*]

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.
dhcp-snooping	(Optional) Display IP source bindings that were learned by DHCP snooping.
static	(Optional) Display static IP source bindings.
interface <i>interface-id</i>	(Optional) Display IP source bindings on a specific interface.
vlan <i>vlan-id</i>	(Optional) Display IP source bindings on a specific VLAN.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(25)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    GigabitEthernet1/0/1
00:00:00:0A:00:0A  11.0.0.2      10000       dhcp-snooping  10    GigabitEthernet1/0/1
```

Related Commands

Command	Description
ip dhcp snooping binding	Configures the DHCP snooping binding database.
ip source binding	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*] [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description

interface <i>interface-id</i>	(Optional) Display IP source guard configuration on a specific interface.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(25)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
-----
Fa1/0/1    ip           active       10.0.0.1        10
Fa1/0/1    ip           active       deny-all       11-20
Fa1/0/2    ip           inactive-trust-port
Fa1/0/3    ip           inactive-no-snooping-vlan
Fa1/0/4    ip-mac       active       10.0.0.2        aaaa.bbbb.cccc  10
Fa1/0/4    ip-mac       active       11.0.0.1        aaaa.bbbb.cccd  11
Fa1/0/4    ip-mac       active       deny-all       deny-all       12-20
Fa1/0/5    ip-mac       active       10.0.0.3        permit-all     10
Fa1/0/5    ip-mac       active       deny-all       permit-all     11-20
```

In the previous example, this is the IP source guard configuration:

- On the Fast Ethernet 1/0/1 interface, 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 exists 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 1/0/2 interface is configured as trusted for DHCP snooping.
- On the Fast Ethernet 1/0/3 interface, DHCP snooping is not enabled on the VLANs to which the interface belongs.
- On the Fast Ethernet 1/0/4 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 1/0/5 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 fastethernet1/0/6
IP source guard is not configured on the interface fa1/0/6.
```

Related Commands

Command	Description
ip verify source	Enables IP source guard on an interface.

show l2protocol-tunnel

Use the **show l2protocol-tunnel** user EXEC command to display information about Layer 2 protocol tunnel ports. The output displays information for the specified interface or all interfaces with protocol tunneling enabled.

show l2protocol-tunnel [*interface interface-id*] [**summary**] [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description	
interface <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 12.
summary	(Optional) Display only Layer 2 protocol summary information.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

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
Fa1/0/1	---	----	----	----	----	----
	---	----	----	----	----	----
	---	----	----	----	----	----
	pagp	----	----	0	242500	
	lacp	----	----	24268	242640	
Fa1/0/2	udld	----	----	0	897960	
	---	----	----	----	----	----
	---	----	----	----	----	----
	pagp	1000	----	24249	242700	
	lacp	----	----	24256	242660	
	udld	----	----	0	897960	

```

Fa1/0/3    cdp          ----    ----    134482    1344820
          ---          ----    ----    ----    ----    ----
          ---          ----    ----    ----    ----    ----
          pagp         1000    ----         0        242500
          lacp          500    ----         0        485320
          udld          300    ----    44899    448980
Fa1/0/4    cdp          ----    ----    134482    1344820
          ---          ----    ----    ----    ----    ----
          ---          ----    ----    ----    ----    ----
          pagp         ----    1000         0        242700
          lacp         ----    ----         0        485220
          udld          300    ----    44899    448980

```

<output truncated>

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
Fa1/0/2	pagp lacp udld	----/----/----	----/----/----	up
Fa1/0/3	pagp lacp udld	1000/----/----	----/----/----	up
Fa1/0/4	pagp lacp udld	1000/ 500/----	----/----/----	up
Fa1/0/5	cdp stp vtp	----/----/----	----/----/----	down
Fa1/0/6	pagp	----/----/----	1000/----/----	down
Fa1/0/7	pagp	----/----/----	1000/----/----	down

Related Commands

Command	Description
clear l2protocol-tunnel counters	Clears counters for protocol tunneling ports.
l2protocol-tunnel	Enables Layer 2 protocol tunneling for Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunking Protocol (VTP) packets on an interface.
l2protocol-tunnel cos	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} [ | {begin | exclude | include} expression]
```

Syntax Description

<i>channel-group-number</i>	(Optional) Number of the channel group. The range is 1 to 12.
counters	Display traffic information.
internal	Display internal information.
neighbor	Display neighbor information.
sys-id	Display the system identifier that is being used by LACP. The system identifier is made up of the LACP system priority and the switch MAC address.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

You can enter any **show lacp** command to display the active channel-group information. To display specific channel information, enter the **show lacp** command with a channel-group number.

If you do not specify a channel group, information for all channel groups appears.

You can enter the *channel-group-number* option to specify a channel group for all keywords except **sys-id**.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show lacp counters** command user EXEC command. [Table 2-23](#) describes the fields in the display.

```
Switch> show lacp counters
      LACPDUs      Marker      Marker Response      LACPDUs
Port      Sent   Recv      Sent   Recv      Sent   Recv      Pkts Err
-----
Channel group:1
Fa1/0/5    19     10         0      0         0      0         0
Fa1/0/6    14      6         0      0         0      0         0
```



```
Fal/0/7      8      7      0      0      0      0      0
```

Table 2-23 *show lacp counters Field Descriptions*

Field	Description
LACPDUs Sent and Recv	The number of LACP packets sent and received by an interface.
Marker Sent and Recv	The number of LACP marker packets sent and received by an interface.
Marker Response Sent and Recv	The number of LACP marker response packets sent and received by an interface.
LACPDUs Pkts and Err	The number of unknown and illegal packets received by LACP for an interface.

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

```
Switch> show lacp 1 internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode           P - Device is in Passive mode

Channel group 1

Port      Flags  State  LACP port  Admin  Oper  Port  Port
          State Priority Key      Key      Number State
Fa1/0/5   SA     bndl   32768     0x3    0x3    0x4    0x3D
Fa1/0/6   SA     bndl   32768     0x3    0x3    0x5    0x3D
Fa1/0/7   SA     bndl   32768     0x3    0x3    0x6    0x3D
```

Table 2-24 describes the fields in the display:

Table 2-24 *show lacp internal Field Descriptions*

Field	Description
State	State of the specific port. These are the allowed values: —Port is in an unknown state. bndl—Port is attached to an aggregator and bundled with other ports. susp—Port is in a suspended state; it is not attached to any aggregator. hot-sby—Port is in a hot-standby state. indiv—Port is incapable of bundling with any other port. indep—Port is in an independent state (not bundled but able to switch data traffic. In this case, LACP is not running on the partner port). down—Port is down.
LACP Port Priority	Port priority setting. LACP uses the port priority to put ports s in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

Table 2-24 *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. The ability of a port to aggregate with other ports is controlled by the port physical characteristics (for example, data rate and duplex capability) and configuration restrictions that you establish.
Oper Key	Runtime operational key that is being used by this port. LACP automatically generates this value as a hexadecimal number.
Port Number	Port number.
Port State	State variables for the port, encoded as individual bits within a single octet with these meanings: • bit0: LACP_Activity • bit1: LACP_Timeout • bit2: Aggregation • bit3: Synchronization • bit4: Collecting • bit5: Distributing • bit6: Defaulted • bit7: Expired Note In the list above, bit7 is the MSB and bit0 is the LSB.

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

Switch> **show lacp neighbor**

Flags: S - Device is sending Slow LACPDUs F - Device is sending Fast LACPDUs
 A - Device is in Active mode P - Device is in Passive mode

Channel group 3 neighbors

Partner's information:

Port	Partner System ID	Partner Port Number	Age	Partner Flags
Fa1/0/3	32768,0007.eb49.5e80	0xC	19s	SP
	LACP Partner Port Priority	Partner Oper Key	Partner Port State	
	32768	0x3	0x3C	

Partner's information:

Port	Partner System ID	Partner Port Number	Age	Partner Flags
Fa1/0/4	32768,0007.eb49.5e80	0xD	15s	SP
	LACP Partner Port Priority	Partner Oper Key	Partner Port State	
	32768	0x3	0x3C	

This is an example of output from the **show lacp sys-id** command:

```
Switch> show lacp sys-id
32765,0002.4b29.3a00
```

The system identification is made up of the system priority and the system MAC address. The first two bytes are the system priority, and the last six bytes are the globally administered individual MAC address associated to the system.

Related Commands

Command	Description
clear lacp	Clears LACP channel-group information.
lacp port-priority	Configures the LACP port priority.
lacp system-priority	Configures the LACP system priority.

show link state group

Use the **show link state group** global configuration command to display the link-state group information.

show link state group [*number*] [**detail**] [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description	<i>number</i>	(Optional) Number of the link-state group.
	detail	(Optional) Specify that detailed information appears.
	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Defaults There is no default.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(25)SEE	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.

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

Examples This is an example of output from the **show link state group 1** command:

```
Switch> show link state group 1
Link State Group: 1      Status: Enabled, Down
```

This is an example of output from the **show link state group detail** command:

```
Switch> show link state group detail
Link State Group: 1 Status: Enabled, Down
Upstream Interfaces : Fa1/0/15(Dwn) Fa1/0/16(Dwn)
Downstream Interfaces : Fa1/0/11(Dis) Fa1/0/12(Dis) Fa1/0/13(Dis) Fa1/0/14(Dis)
```

```
Link State Group: 2 Status: Enabled, Down
Upstream Interfaces : Fa1/0/15(Dwn) Fa1/0/16(Dwn) Fa1/0/17(Dwn)
Downstream Interfaces : Fa1/0/11(Dis) Fa1/0/12(Dis) Fa1/0/13(Dis) Fa1/0/14(Dis)
(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
```

Related Commands

Command	Description
link state group	Configures an interface as a member of a link-state group.
link state track	Enables a link-state group.
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_comm_and_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.

show location

Use the **show location** user EXEC command to display location information for an endpoint.

```
show location admin-tag [ [ {begin | exclude | include} expression]

show location civic-location {identifier id number | interface interface-id | static } | {begin |
exclude | include} expression]

show location elin-location {identifier id number | interface interface-id | static} | {begin |
exclude | include} expression]
```

Syntax Description

admin-tag	Display administrative tag or site information.
civic-location	Display civic location information.
elin-location	Display emergency location information (ELIN).
identifier id	Specify the ID for the civic location or the elin location. The id range is 1 to 4095.
interface interface-id	(Optional) Display location information for the specified interface or all interfaces. Valid interfaces include physical ports.
static	Display static configuration information.
begin	(Optional) Display begins with the line that matches the expression.
exclude	(Optional) Display excludes lines that match the expression.
include	(Optional) Display includes lines that match the specified expression.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(40)SE	This command was introduced.

Usage Guidelines

Use the **show location** command to display location information for an endpoint.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show location civic-location** command that displays location information for an interface:

```
Switch> show location civic interface g2/0/1
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
location (global configuration)	Configures the global location information for an endpoint.
location (interface configuration)	Configures the location information for an interface.

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*] [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface <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 64.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC; the **interface** keyword is available only in privileged EXEC mode.

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show mac-access group** command. In this display, Fast Ethernet interface 1/0/12 has the MAC access list *macl_e1* applied; no MAC ACLs are applied to other interfaces.

```
Switch> show mac access-group
Interface FastEthernet1/0/1:
  Inbound access-list is not set
Interface FastEthernet1/0/2:
  Inbound access-list is macl_e1
Interface FastEthernet1/0/3:
  Inbound access-list is not set
Interface FastEthernet1/0/4:
  Inbound access-list is not set

<output truncated>

Interface FastEthernet1/0/10:
  Inbound access-list is not set
Interface FastEthernet1/0/11:
  Inbound access-list is not set
Interface FastEthernet1/0/12:
  Inbound access-list is macl_e1

<output truncated>
```


This is an example of output from the **show mac access-group interface** *interface-id* command:

```
Switch# show mac access-group interface gigabitEthernet1/0/2
Interface GigabitEthernet1/0/2:
  Inbound access-list is mac1_e1
```

Related Commands

Command	Description
mac access-group	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 [ | {begin | exclude | include} expression]
```

Syntax Description	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

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
----    -
A11     0000.0000.0001   STATIC  CPU
A11     0000.0000.0002   STATIC  CPU
A11     0000.0000.0003   STATIC  CPU
A11     0000.0000.0009   STATIC  CPU
A11     0000.0000.0012   STATIC  CPU
A11     0180.c200.000b   STATIC  CPU
A11     0180.c200.000c   STATIC  CPU
A11     0180.c200.000d   STATIC  CPU
A11     0180.c200.000e   STATIC  CPU
A11     0180.c200.000f   STATIC  CPU
A11     0180.c200.0010   STATIC  CPU
1       0030.9441.6327   DYNAMIC Fa1/0/23
Total Mac Addresses for this criterion: 12
```

Related Commands	Command	Description
	clear mac address-table dynamic	Deletes from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, or all dynamic addresses on a particular VLAN.
	show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
	show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
	show mac address-table dynamic	Displays dynamic MAC address table entries only.
	show mac address-table interface	Displays the MAC address table information for the specified interface.
	show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
	show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
	show mac address-table static	Displays static MAC address table entries only.
	show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table address

Use the **show mac address-table address** user EXEC command to display MAC address table information for the specified MAC address.

show mac address-table address *mac-address* [**interface** *interface-id*] [**vlan** *vlan-id*] [**|** { **begin** | **exclude** | **include** } *expression*]

Syntax Description		
<i>mac-address</i>		Specify the 48-bit MAC address; the valid format is H.H.H.
interface <i>interface-id</i>		(Optional) Display information for a specific interface. Valid interfaces include physical ports and port channels.
vlan <i>vlan-id</i>		(Optional) Display entries for the specific VLAN only. The range is 1 to 4094.
 begin		(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude		(Optional) Display excludes lines that match the <i>expression</i> .
 include		(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>		Expression in the output to use as a reference point.

Command Modes User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples This is an example of output from the **show mac address-table address** command:

```
Switch# show mac address-table address 0002.4b28.c482
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
All     0002.4b28.c482  STATIC  CPU
Total Mac Addresses for this criterion: 1
```

Related Commands	Command	Description
	show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
	show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
	show mac address-table dynamic	Displays dynamic MAC address table entries only.

Command	Description
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table aging-time

Use the **show mac address-table aging-time** user EXEC command to display the aging time of a specific address table instance, all address table instances on a specified VLAN or, if a specific VLAN is not specified, on all VLANs.

```
show mac address-table aging-time [vlan vlan-id] [ | { begin | exclude | include } expression]
```

Syntax Description	vlan <i>vlan-id</i>	(Optional) Display aging time information for a specific VLAN. The range is 1 to 4094.
	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines If no VLAN number is specified, the aging time for all VLANs appears. Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples This is an example of output from the **show mac address-table aging-time** command:

```
Switch> show mac address-table aging-time
Vlan      Aging Time
----      -
1         300
```

This is an example of output from the **show mac address-table aging-time vlan 10** command:

```
Switch> show mac address-table aging-time vlan 10
Vlan      Aging Time
----      -
10        300
```

Related Commands

Command	Description
mac address-table aging-time	Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated.
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table count

Use the **show mac address-table count** user EXEC command to display the number of addresses present in all VLANs or the specified VLAN.

```
show mac address-table count [vlan vlan-id] [ | {begin | exclude | include} expression]
```

Syntax Description	vlan vlan-id	(Optional) Display the number of addresses for a specific VLAN. The range is 1 to 4094.
	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	expression	Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines

If no VLAN number is specified, the address count for all VLANs appears.

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

Examples

This is an example of output from the **show mac address-table count** command:

```
Switch# show mac address-table count

Mac Entries for Vlan 10:
-----
Dynamic Address Count   : 0
Static Address Count    : 0
Total Mac Addresses     : 0

Mac Entries for Vlan 1:
-----
Dynamic Address Count   : 10
Static Address Count    : 0
Total Mac Addresses     : 10

Total Mac Address Space Available: 6120
```


Related Commands

Command	Description
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table dynamic

Use the **show mac address-table dynamic** user EXEC command to display only dynamic MAC address table entries.

```
show mac address-table dynamic [address mac-address] [interface interface-id] [vlan vlan-id]
[ | { begin | exclude | include } expression]
```

Syntax Description

address <i>mac-address</i>	(Optional) Specify a 48-bit MAC address; the valid format is H.H.H (available in privileged EXEC mode only).
interface <i>interface-id</i>	(Optional) Specify an interface to match; valid <i>interfaces</i> include physical ports and port channels.
vlan <i>vlan-id</i>	(Optional) Display entries for a specific VLAN; the range is 1 to 4094.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC; **address** keyword available only in privileged EXEC mode.

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show mac address-table dynamic** command:

```
Switch> show mac address-table dynamic
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
1       0000.0c07.ac00   DYNAMIC Fa1/0/1
1       0000.0c07.ac81   DYNAMIC Fa1/0/1
1       0004.5a5e.f635   DYNAMIC Fa1/0/1
1       0006.d713.8dd0   DYNAMIC Fa1/0/1
1       0006.d78b.5d80   DYNAMIC Fa1/0/1
1       0008.217a.ea00   DYNAMIC Fa1/0/1
1       000a.b7d1.6f5b   DYNAMIC Fa1/0/1
1       0010.7b3a.e967   DYNAMIC Fa1/0/1
1       0010.a4e6.6e58   DYNAMIC Fa1/0/1
1       0090.92cf.1400   DYNAMIC Fa1/0/1
Total Mac Addresses for this criterion: 10
```

Related Commands

Command	Description
clear mac address-table dynamic	Deletes from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, or all dynamic addresses on a particular VLAN.
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table interface

Use the **show mac address-table interface** user command to display the MAC address table information for the specified interface in the specified VLAN.

```
show mac address-table interface interface-id [vlan vlan-id] [ | { begin | exclude | include } expression ]
```

Syntax Description		
<i>interface-id</i>		Specify an interface type; valid <i>interfaces</i> include <i>physical ports</i> and <i>port channels</i> .
vlan <i>vlan-id</i>		(Optional) Display entries for a specific VLAN; the range is 1 to 4094.
 begin		(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude		(Optional) Display excludes lines that match the <i>expression</i> .
 include		(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>		Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

Examples	This is an example of output from the show mac address-table interface <i>interface-id</i> command:

```
Switch> show mac address-table interface fastethernet1/0/2
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
1       0030.b635.7862   DYNAMIC Fa1/0/2
1       00b0.6496.2741   DYNAMIC Fa1/0/2
Total Mac Addresses for this criterion: 2
```

Related Commands	Command	Description
	show mac address-table address	Displays MAC address table information for the specified MAC address.
	show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
	show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.

Command	Description
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table 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*] [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description	vlan <i>vlan-id</i>	(Optional) Display information for a specific VLAN. The range is 1 to 4094.
	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.2(25)SEG	This command was introduced.

Usage Guidelines

Use the **show mac address-table learning** command without any keywords to display configured VLANs and whether MAC address learning is enabled or disabled on them. The default is that MAC address learning is enabled on all VLANs. Use the command with a specific VLAN ID to display the learning status on an individual VLAN.

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mac address-table learning** 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
```

Related Commands	Command	Description
	mac address-table learning vlan	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 [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description	begin	(Optional) Display begins with the line that matches the expression.
	exclude	(Optional) Display excludes lines that match the expression.
	include	(Optional) Display includes lines that match the specified expression.
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.2(25)SED	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain output do not appear, but the lines that contain <i>Output</i> appear.

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#
```

 show mac address-table move update

Related Commands	Command	Description
	clear mac address-table move update	Clears the MAC address-table move update counters.
	mac address-table move update	Configures MAC address-table move update on the switch.

show mac address-table multicast

Use the **show mac address-table multicast** user EXEC command to display the Layer 2 multicast entries for all VLANs. Use the command in privileged EXEC mode to display specific multicast entries.

```
show mac address-table multicast [vlan-id] [count | user [count]] [ | {begin | exclude | include}
expression]
```

Syntax Description		
vlan <i>vlan-id</i>	(Optional) Display addresses for a specific VLAN. The range is 1 to 4094.	
count	(Optional) Display the total number of entries for the specified command options instead of the actual entries.	
user	(Optional) Display only the user-configured multicast entries.	
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .	
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .	
 include	(Optional) Display includes lines that match the specified <i>expression</i> .	
<i>expression</i>	Expression in the output to use as a reference point.	



Note

Though visible in the command-line help string, the **igmp-snooping** keyword is not supported. Use the **show ip source binding** privileged EXEC command to display the Internet Group Management Protocol (IGMP) snooping multicast table.

Command Modes	User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

Examples	This is an example of output from the show mac address-table multicast command. It shows how to display all multicast entries for the switch.

```
Switch> show mac address-table multicast
Vlan    Mac Address      Type    Ports
----    -
1       0100.5e00.0128   IGMP    Gi1/0/1
```

This is an example of output from the **show mac address-table multicast count** command. It shows how to display a total count of MAC address entries for the switch.

```
Switch> show mac address-table multicast count
Multicast MAC Entries for all vlans:    10
```

This is an example of output from the **show mac address-table multicast vlan 1 count** command. It shows how to display a total count of MAC address entries for a VLAN.

```
Switch> show mac address-table multicast vlan 1 count
Multicast MAC Entries for vlan 1:    4
```

Related Commands	Command	Description
	show mac address-table address	Displays MAC address table information for the specified MAC address.
	show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
	show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
	show mac address-table dynamic	Displays dynamic MAC address table entries only.
	show mac address-table interface	Displays the MAC address table information for the specified interface.
	show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
	show mac address-table static	Displays static MAC address table entries only.
	show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table 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 [**interface** *interface-id*] [**|** { **begin** | **exclude** | **include** } *expression*]

Syntax Description		
interface	(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.	
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .	
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .	
 include	(Optional) Display includes lines that match the specified <i>expression</i> .	
<i>expression</i>	Expression in the output to use as a reference point.	

Command Modes	User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	Use the show mac address-table notification command without any keywords to display whether the 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 flags for all interfaces. If the <i>interface-id</i> is included, only the flags for that interface are displayed. Expressions are case sensitive. For example, if you enter exclude output, the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

Examples	This is an example of output from the show mac address-table notification command:

```
Switch> show mac address-table notification
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 :
```

show mac address-table notification

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
clear mac address-table notification	Clears the MAC address notification global counters.
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table static

Use the **show mac address-table static** user EXEC command to display only static MAC address table entries.

```
show mac address-table static [address mac-address] [interface interface-id] [vlan vlan-id]
[ | {begin | exclude | include} expression]
```

Syntax Description	
address <i>mac-address</i>	(Optional) Specify a 48-bit MAC address; the valid format is H.H.H (available in privileged EXEC mode only).
interface <i>interface-id</i>	(Optional) Specify an interface to match; valid <i>interfaces</i> include physical ports and port channels.
vlan <i>vlan-id</i>	(Optional) Display addresses for a specific VLAN. The range is 1 to 4094.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes User EXEC; **address** keyword available only in privileged EXEC mode.

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples This is an example of output from the **show mac address-table static** command:

```
Switch> show mac address-table static

      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
All     0100.0ccc.cccc   STATIC  CPU
All     0180.c200.0000   STATIC  CPU
All     0100.0ccc.cccd   STATIC  CPU
All     0180.c200.0001   STATIC  CPU
All     0180.c200.0004   STATIC  CPU
All     0180.c200.0005   STATIC  CPU
4       0001.0002.0004   STATIC  Drop
6       0001.0002.0007   STATIC  Drop
Total Mac Addresses for this criterion: 8
```

■ show mac address-table static

Related Commands	Command	Description
	mac address-table static	Adds static addresses to the MAC address table.
	show mac address-table address	Displays MAC address table information for the specified MAC address.
	show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
	show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
	show mac address-table dynamic	Displays dynamic MAC address table entries only.
	show mac address-table interface	Displays the MAC address table information for the specified interface.
	show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
	show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
	show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table vlan

Use the **show mac address-table vlan** user EXEC command to display the MAC address table information for the specified VLAN.

show mac address-table vlan *vlan-id* [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description	<i>vlan-id</i>	(Optional) Display addresses for a specific VLAN. The range is 1 to 4094.
	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

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.c200.0004   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: 10
```

Related Commands	Command	Description
	show mac address-table address	Displays MAC address table information for the specified MAC address.
	show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
	show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
	show mac address-table dynamic	Displays dynamic MAC address table entries only.
	show mac address-table interface	Displays the MAC address table information for the specified interface.
	show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
	show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
	show mac address-table static	Displays static MAC address table entries only.

show mls qos

Use the **show mls qos** user EXEC command to display global quality of service (QoS) configuration information.

show mls qos [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

Examples	This is an example of output from the show mls qos command when QoS is enabled and Differentiated Services Code Point (DSCP) transparency is disabled:

```
Switch> show mls qos
QoS is enabled
QoS ip packet dscp rewrite disabled
```

This is an example of output from the **show mls qos** command when QoS is enabled and DSCP transparency is enabled:

```
Switch> show mls qos
QoS is enabled
QoS ip packet dscp rewrite enabled
```

Related Commands	Command	Description
	mls qos	Enables QoS for the entire switch.

show mls qos aggregate-policer

Use the **show mls qos aggregate-policer** user EXEC command to display the quality of service (QoS) aggregate policer configuration. 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.

```
show mls qos aggregate-policer [aggregate-policer-name] [ | {begin | exclude | include}
expression]
```

Syntax Description	<i>aggregate-policer-name</i>	(Optional) Display the policer configuration for the specified name.
	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples This is an example of output from the **show mls qos aggregate-policer** command:

```
Switch> show mls qos aggregate-policer policer1
aggregate-policer policer1 88000 2000000 exceed-action drop
Not used by any policy map
```

Related Commands	Command	Description
	mls qos aggregate-policer	Defines policer parameters that can be shared by multiple classes within the same policy map.

show mls qos input-queue

Use the **show mls qos input-queue** user EXEC command to display quality of service (QoS) settings for the ingress queues.

show mls qos input-queue [**|** { **begin** | **exclude** | **include** } *expression*]

Syntax Description	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

Examples This is an example of output from the **show mls qos input-queue** command:

```
Switch> show mls qos input-queue
Queue      :      1      2
-----
buffers    :      90     10
bandwidth  :       4      4
priority   :       0     10
threshold1 :     100    100
threshold2 :     100    100
```

Related Commands	Command	Description
	mls qos srr-queue input bandwidth	Assigns shaped round robin (SRR) weights to an ingress queue.
	mls qos srr-queue input buffers	Allocates the buffers between the ingress queues.
	mls qos srr-queue input cos-map	Maps class of service (CoS) values to an ingress queue or assigns CoS values to a queue and to a threshold ID.
	mls qos srr-queue input dscp-map	Maps Differentiated Services Code Point (DSCP) values to an ingress queue or assigns DSCP values to a queue and to a threshold ID.

 show mls qos input-queue

Command	Description
mls qos srr-queue input priority-queue	Configures the ingress priority queue and guarantees bandwidth.
mls qos srr-queue input threshold	Assigns weighted tail-drop (WTD) threshold percentages to an ingress queue.

show mls qos interface

Use the **show mls qos interface** user EXEC command to display quality of service (QoS) information at the port level.

show mls qos interface [*interface-id*] [**buffers** | **queueing** | **statistics**]
[| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

<i>interface-id</i>	(Optional) Display QoS information for the specified port. Valid interfaces include physical ports.
buffers	(Optional) Display the buffer allocation among the queues.
queueing	(Optional) Display the queueing strategy (shared or shaped) and the weights corresponding to the queues.
statistics	(Optional) Display statistics for sent and received Differentiated Services Code Point (DSCP) and class of service (CoS) values, the number of packets queued or dropped, and the number of in-profile and out-of-profile packets for each policer.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.



Note

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

Command Modes

User EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show mls qos interface** *interface-id* command:

```
Switch# show mls qos interface fastethernet1/0/7
FastEthernet1/0/7
Attached policy-map for Ingress: videowizard_policy
trust state: not trusted
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
```

show mls qos interface

This is an example of output from the **show mls qos interface *interface-id* buffers** command:

```
Switch> show mls qos interface fastethernet1/0/7 buffers
FastEthernet1/0/7
The port is mapped to qset : 1
The allocations between the queues are : 25 25 25 25
```

This is an example of output from the **show mls qos interface *interface-id* queueing** command:

```
Switch> show mls qos interface fastethernet1/0/7 queueing
GigabitEthernet1/0/7
Egress Priority Queue :enabled
Shaped queue weights (absolute) : 25 0 0 0
Shared queue weights : 25 25 25 25
The port bandwidth limit : 100 (Operational Bandwidth:100.0)
The port is mapped to qset : 1
```

This is an example of output from the **show mls qos interface *interface-id* statistics** command. [Table 2-25](#) describes the fields in this display.

```
Switch> show mls qos interface fastethernet1/0/7 statistics
FastEthernet1/0/7

dscp: incoming
-----
 0 - 4 :      4213      0      0      0      0
 5 - 9 :         0      0      0      0      0
10 - 14 :        0      0      0      0      0
15 - 19 :        0      0      0      0      0
20 - 24 :        0      0      0      0      0
25 - 29 :        0      0      0      0      0
30 - 34 :        0      0      0      0      0
35 - 39 :        0      0      0      0      0
40 - 44 :        0      0      0      0      0
45 - 49 :        0      0      0      6      0
50 - 54 :        0      0      0      0      0
55 - 59 :        0      0      0      0      0
60 - 64 :        0      0      0      0      0
dscp: outgoing
-----
 0 - 4 :     363949      0      0      0      0
 5 - 9 :         0      0      0      0      0
10 - 14 :        0      0      0      0      0
15 - 19 :        0      0      0      0      0
20 - 24 :        0      0      0      0      0
25 - 29 :        0      0      0      0      0
30 - 34 :        0      0      0      0      0
35 - 39 :        0      0      0      0      0
40 - 44 :        0      0      0      0      0
45 - 49 :        0      0      0      0      0
50 - 54 :        0      0      0      0      0
55 - 59 :        0      0      0      0      0
60 - 64 :        0      0      0      0      0
cos: incoming
-----
 0 - 4 :     132067      0      0      0      0
 5 - 9 :         0      0      0      0      0
cos: outgoing
-----
 0 - 4 :     739155      0      0      0      0
```

```
5 - 9 :          90          0          0
```

```
Policer: Inprofile:          0 OutofProfile:          0
```

**Note**

The **show mls qos interface *interface-id* statistics** command output might show more throughput than the actual amount on the interface.

Table 2-25 *show mls qos interface statistics Field Descriptions*

Field		Description
DSCP	incoming	Number of received packets for each DSCP value.
	outgoing	Number of sent packets for each DSCP value.
CoS	incoming	Number of received packets for each CoS value.
	outgoing	Number of sent packets for each CoS value.
Policer	Inprofile	Number of in profile packets for each policer.
	Outofprofile	Number of out of profile packets for each policer.

Related Commands

Command	Description
mls qos queue-set output buffers	Allocates buffers to a queue-set.
mls qos queue-set output threshold	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
mls qos srr-queue input bandwidth	Assigns shaped round robin (SRR) weights to an ingress queue.
mls qos srr-queue input buffers	Allocates the buffers between the ingress queues.
mls qos srr-queue input cos-map	Maps CoS values to an ingress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue input dscp-map	Maps DSCP values to an ingress queue or maps DSCP values to a queue and to a threshold ID.
mls qos srr-queue input priority-queue	Configures the ingress priority queue and guarantees bandwidth.
mls qos srr-queue input threshold	Assigns WTD threshold percentages to an ingress queue.
mls qos srr-queue output cos-map	Maps CoS values to an egress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue output dscp-map	Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
priority-queue	Enables the egress priority queue on a port.
queue-set	Maps a port to a queue-set.
srr-queue bandwidth limit	Limits the maximum output on a standard port.
srr-queue bandwidth shape	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a standard port.
srr-queue bandwidth share	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

show mls qos maps

Use the **show mls qos maps** user EXEC command to display quality of service (QoS) mapping information. During classification, QoS uses the mapping tables to represent the priority of the traffic and to derive a corresponding class of service (CoS) or Differentiated Services Code Point (DSCP) value from the received CoS, DSCP, or IP precedence value.

```
show mls qos maps [cos-dscp | cos-input-q | cos-output-q | dscp-cos | dscp-input-q |
dscp-mutation dscp-mutation-name | dscp-output-q | ip-prec-dscp | policed-dscp] [ | {begin
| exclude | include} expression]
```

Syntax Description		
cos-dscp	(Optional)	Display class of service (CoS)-to-DSCP map.
cos-input-q	(Optional)	Display the CoS input queue threshold map.
cos-output-q	(Optional)	Display the CoS output queue threshold map.
dscp-cos	(Optional)	Display DSCP-to-CoS map.
dscp-input-q	(Optional)	Display the DSCP input queue threshold map.
dscp-mutation <i>dscp-mutation-name</i>	(Optional)	Display the specified DSCP-to-DSCP-mutation map.
dscp-output-q	(Optional)	Display the DSCP output queue threshold map.
ip-prec-dscp	(Optional)	Display the IP-precedence-to-DSCP map.
policed-dscp	(Optional)	Display the policed-DSCP map.
 begin	(Optional)	Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional)	Display excludes lines that match the <i>expression</i> .
 include	(Optional)	Display includes lines that match the specified <i>expression</i> .
<i>expression</i>		Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

The policed-DSCP, DSCP-to-CoS, and the DSCP-to-DSCP-mutation maps are displayed as a matrix. The d1 column specifies the most-significant digit in the DSCP. The d2 row specifies the least-significant digit in the DSCP. The intersection of the d1 and d2 values provides the policed-DSCP, the CoS, or the mutated-DSCP value. For example, in the DSCP-to-CoS map, a DSCP value of 43 corresponds to a CoS value of 5.

The DSCP input queue threshold and the DSCP output queue threshold maps are displayed as a matrix. The d1 column specifies the most-significant digit of the DSCP number. The d2 row specifies the least-significant digit in the DSCP number. The intersection of the d1 and the d2 values provides the queue ID and threshold ID. For example, in the DSCP input queue threshold map, a DSCP value of 43 corresponds to queue 2 and threshold 1 (02-01).

The CoS input queue threshold and the CoS output queue threshold maps show the CoS value in the top row and the corresponding queue ID and threshold ID in the second row. For example, in the CoS input queue threshold map, a CoS value of 5 corresponds to queue 2 and threshold 1 (2-1).

Examples

This is an example of output from the **show mls qos maps** command:

```
Switch> show mls qos maps
```

```
Policed-dscp map:
```

```

d1 : d2 0  1  2  3  4  5  6  7  8  9
-----
0 :   00 01 02 03 04 05 06 07 08 09
1 :   10 11 12 13 14 15 16 17 18 19
2 :   20 21 22 23 24 25 26 27 28 29
3 :   30 31 32 33 34 35 36 37 38 39
4 :   40 41 42 43 44 45 46 47 48 49
5 :   50 51 52 53 54 55 56 57 58 59
6 :   60 61 62 63

```

```
Dscp-cos map:
```

```

d1 : d2 0  1  2  3  4  5  6  7  8  9
-----
0 :   00 00 00 00 00 00 00 00 01 01
1 :   01 01 01 01 01 01 02 02 02 02
2 :   02 02 02 02 03 03 03 03 03 03
3 :   03 03 04 04 04 04 04 04 04 04
4 :   05 05 05 05 05 05 05 05 06 06
5 :   06 06 06 06 06 06 07 07 07 07
6 :   07 07 07 07

```

```
Cos-dscp map:
```

```

cos:  0  1  2  3  4  5  6  7
-----
dscp:  0  8 16 24 32 40 48 56

```

```
IpPrecedence-dscp map:
```

```

ipprec:  0  1  2  3  4  5  6  7
-----
dscp:    0  8 16 24 32 40 48 56

```

```
Dscp-outputq-threshold map:
```

```

d1 :d2    0    1    2    3    4    5    6    7    8    9
-----
0 :   02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01
1 :   02-01 02-01 02-01 02-01 02-01 02-01 02-01 03-01 03-01 03-01
2 :   03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01
3 :   03-01 03-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01
4 :   01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 04-01
5 :   04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01
6 :   04-01 04-01 04-01 04-01

```

```
Dscp-inputq-threshold map:
```

```

d1 :d2    0    1    2    3    4    5    6    7    8    9
-----
0 :   01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
1 :   01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
2 :   01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01

```

show mls qos maps

```

3 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
4 :    02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 01-01
5 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
6 :    01-01 01-01 01-01 01-01

```

Cos-outputq-threshold map:

```
cos:  0   1   2   3   4   5   6   7
```

```
-----
queue-threshold: 2-1 2-1 3-1 3-1 4-1 1-1 4-1 4-1

```

Cos-inputq-threshold map:

```
cos:  0   1   2   3   4   5   6   7
```

```
-----
queue-threshold: 1-1 1-1 1-1 1-1 1-1 2-1 1-1 1-1

```

Dscp-dscp mutation map:

Default DSCP Mutation Map:

```
d1 :  d2 0   1   2   3   4   5   6   7   8   9
```

```
-----
0 :    00 01 02 03 04 05 06 07 08 09
1 :    10 11 12 13 14 15 16 17 18 19
2 :    20 21 22 23 24 25 26 27 28 29
3 :    30 31 32 33 34 35 36 37 38 39
4 :    40 41 42 43 44 45 46 47 48 49
5 :    50 51 52 53 54 55 56 57 58 59
6 :    60 61 62 63

```

Related Commands

Command	Description
mls qos map	Defines the CoS-to-DSCP map, the DSCP-to-CoS map, the DSCP-to-DSCP-mutation map, the IP-precedence-to-DSCP map, and the policed-DSCP map.
mls qos srr-queue input cos-map	Maps CoS values to an ingress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue input dscp-map	Maps DSCP values to an ingress queue or maps DSCP values to a queue and to a threshold ID.
mls qos srr-queue output cos-map	Maps CoS values to an egress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue output dscp-map	Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID.

show mls qos queue-set

Use the **show mls qos queue-set** user EXEC command to display quality of service (QoS) settings for an egress queue-set.

show mls qos queue-set [*qset-id*] [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description	<i>qset-id</i>	(Optional) ID of the queue-set. Each port belongs to a queue-set, which defines all the characteristics of the four egress queues per port. The range is 1 to 2.
	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

Examples	This is an example of output from the show mls qos queue-set command:

```
Switch> show mls qos queue-set
Queueset: 1
Queue   :      1      2      3      4
-----
buffers  :      25      25      25      25
threshold1:    100     200     100     100
threshold2:    100     200     100     100
reserved  :      50      50      50      50
maximum  :     400     400     400     400
Queueset: 2
Queue   :      1      2      3      4
-----
buffers  :      25      25      25      25
threshold1:    100     200     100     100
threshold2:    100     200     100     100
reserved  :      50      50      50      50
maximum  :     400     400     400     400
```

 show mls qos queue-set

Related Commands	Command	Description
	mls qos queue-set output buffers	Allocates buffers to the queue-set.
	mls qos queue-set output threshold	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation of the queue-set.

show mls qos vlan

Use the **show mls qos vlan** user EXEC command to display the policy maps attached to a switch virtual interface (SVI).

show mls qos vlan *vlan-id* [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description

<i>vlan-id</i>	Display the policy maps for the specified VLAN. The range is 1 to 4094.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(25)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mls qos queue-set** command:

```
Switch> show mls qos vlan 10
Vlan10
Attached policy-map for Ingress:pm-test-pm-2
```

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to multiple ports and enters policy-map configuration mode.

show monitor

Use the **show monitor** user EXEC command to display information about all Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) sessions on the switch. Use the command with keywords to show a specific session, all sessions, all local sessions, or all remote sessions.

show monitor [**session** { *session_number* | **all** | **local** | **range** *list* | **remote** } [**detail**]] [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description

session	(Optional) Display information about specified SPAN sessions.
<i>session_number</i>	Specify the number of the SPAN or RSPAN session. The range is 1 to 66.
all	Display all SPAN sessions.
local	Display only local SPAN sessions.
range <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. Note This keyword is available only in privileged EXEC mode.
remote	Display only remote SPAN sessions.
detail	(Optional) Display detailed information about the specified sessions.
begin	Display begins with the line that matches the <i>expression</i> .
exclude	Display excludes lines that match the <i>expression</i> .
include	Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

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

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** command:

```
Switch# show monitor
Session 1
-----
Type : Local Session
Source Ports :
RX Only : Fa1/0/1
Both : Fa1/0/2-3, Fa1/0/5-6
```

```

Destination Ports : Fa1/0/20
Encapsulation : Replicate
Ingress : Disabled

```

```

Session 2
-----
Type : Remote Source Session
Source VLANs :
TX Only : 10
Both : 1-9
Dest RSPAN VLAN : 105

```

This is an example of output for the **show monitor** command for RSPAN source session 1:

```

Switch# show monitor session 1
Session 1
-----
Type : Local Session
Source Ports :
RX Only : Fa1/0/1
Both : Fa1/0/2-3, Fa1/0/5-6
Destination Ports : Fa1/0/20
Encapsulation : Replicate
Ingress : Disabled

```

This is an example of output for the **show monitor session all** command when ingress traffic forwarding is enabled:

```

Switch# show monitor session all
Session 1
-----
Type : Local Session
Source Ports :
Both : Fa1/0/2
Destination Ports : Fa1/0/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encap : DOT1Q

Session 2
-----
Type : Local Session
Source Ports :
Both : Fa1/0/8
Destination Ports : Fa1/0/12
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged

```

Related Commands

Command	Description
monitor session	Starts or modifies a SPAN or RSPAN session.

show mpls l2transport vc

Use the **show mpls l2transport vc** user EXEC command to provide information about the Ethernet over multiprotocol label switching (EoMPLS) virtual circuits (VCs) that have been enabled to route Layer 2 packets on a provider-edge device.

```
show mpls l2transport vc [detail] [summary] [vc-id] [vc-id-min - vc-id-max] [ | { begin | exclude | include } expression]
```

Syntax Description	detail	(Optional) Display provides detailed information about the VCs on a provider-edge device.
	summary	(Optional) Display provides a summary of the configured VCs on the provider-edge device MPLS interfaces.
	vcid	(Optional) Display information about the specified VC. The range is 1 to 4294967295.
	vc-id-min - vc-id-max	(Optional) Display information about the specified range of VCs. The range is 1 to 4294967295.
	begin	Display begins with the line that matches the <i>expression</i> .
	exclude	Display excludes lines that match the <i>expression</i> .
	include	Display includes lines that match the specified <i>expression</i> .
	expression	Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples This is an example of output from the **show mpls l2transport vc** command:

```
Switch> show mpls l2transport vc
Transport Client      VC      Trans Local      Remote      Tunnel
VC ID      Intf      State  Type  VC Label  VC Label  Label
49          V160      UP     vlan  18        18        implc-null
50          V180      DOWN   vlan  unassigned unassigned not ready
52          Fa1/0/2    UP     ether 17        17        implc-null
```

Table 2-26 describes the fields in the display.

Table 2-26 *show mpls l2 transport vc Field Descriptions*

Field	Description
Transport VC ID	The virtual circuit identifier assigned to one of the interfaces on the device.
Client Intf	The ingress or egress interface through which the Layer 2 VLAN packet travels. The interface is a VLAN or a physical interface.
VC State	The state of the VC (UP or DOWN): UP—The VC can carry traffic between the two VC end points. A VC is up when both the local and remote interfaces are programmed. - The local interface is programmed if the VC is configured and the client interface is up. - The remote interface is programmed if the remote interface is configured and there is a VC remote VC label and an IGP label. The IGP label means that there is a label-switched path (LSP) to the peer. DOWN—The VC is not ready to carry traffic between the two VC end points.
Trans Type	The forwarding mode used.
Local VC Label	The VC label that a device signals to its peer device. The local VC label determines the egress interface of a packet arriving from the MPLS backbone.
Remote VC Label	The VC label of the remote peer device.
Tunnel Label	An IGP label used to route the packet over the MPLS backbone to the destination device that has the egress interface.

This is an example of the output from the **show mpls l2transport vc summary** command:

```
Switch> show mpls l2transport vc summary
MPLS interface VC summary (active vc(s) only):

VC summary (active/non-active) by destination:
  destination: 172.22.255.255, Number of locally configured vc(s): 2
```

This is an example of the output from the **show mpls l2transport vc detail** command:

```
Switch> show mpls l2transport vc detail
vcid: 49, type: vlan , local groupid: 32, remote groupid: 36 (vc is up)
client: Vl60 is up, destination: 192.168.255.255, Peer LDP Ident: 192.168.255.25:0
local label: 18, remote label: 18, tunnel label: implc-null
outgoing interface: Gi1/1/1, next hop: 10.2.0.2
Local MTU: 1500, Remote MTU: 1500
Remote interface description: Vlan60
Packet totals(in/out): 0/0
byte totals(in/out): 0/0

vcid: 50, type: vlan , local groupid: 33, remote groupid: -1 (vc is down)
client: Vl80 is not up, destination: 192.168.255.255, Peer LDP Ident: 192.168.255.255:0
local label: unassigned, remote label: unassigned, tunnel label: not ready
Local MTU: 1500, Remote MTU: 0
```

show mpls l2transport vc

```

Remote interface description:
Packet totals(in/out): 0/0
byte totals(in/out): 0/0

vcid: 52, type: ether , local groupid: 3, remote groupid: 3 (vc is up)
client: Fa1/0/2 is up, destination: 192.168.255.255, Peer LDP Ident: 192.168.255
.255:0
local label: 17, remote label: 17, tunnel label: implc-null
outgoing interface: Gi1/1/1, next hop: 10.2.0.2
Local MTU: 1500, Remote MTU: 1500
Remote interface description: FastEthernet1/0/2
Packet totals(in/out): 606955/0
byte totals(in/out): 47342490/0

```

Table 2-27 describes the fields in the display.

Table 2-27 *show mpls l2 transport vc detail Field Descriptions*

Field	Description
vcid	The virtual circuit identifier assigned to one of the interfaces on the device.
type	The forwarding mode used.
local groupid	The ID used to group VCs locally. EoMPLS groups VCs by the hardware port, which is unique for each port on a device.
remote groupid	The ID used by the peer to group several VCs.
vc is up or vc is down	The state of the VC (up or down): Up—The VC can carry traffic between the two VC end points. A VC is up when both the local and remote interfaces are programmed. - The local interface is programmed if the VC is configured and the client interface is up. - The remote interface is programmed if the remote interface is configured and there is a VC remote VC label and an IGP label. The IGP label means that there is a label-switched path (LSP) to the peer. Down—The VC is not ready to carry traffic between the two VC end points.
client	The ingress or egress interface through which the Layer 2 VLAN packet travels. The interface is a VLAN or physical interface.
destination	The destination specified for this VC. You specify the destination IP address as part of the mpls l2transport route interface configuration command.
Peer LDP Ident	The LDP IP address of the targeted peer.
local label	The VC label that a device signals to its peer device. The local VC label determines the egress interface of a packet arriving from the MPLS backbone.
remote label	The VC label of the remote peer device.
tunnel label	An IGP label used to route the packet over the MPLS backbone to the destination device with the egress interface.
Outgoing interface	The egress interface of the VC.

Table 2-27 *show mpls l2 transport vc detail Field Descriptions (continued)*

Field	Description
Next hop	The IP address of the next hop.
Local MTU	The maximum transmission unit specified for the client interface.
Remote MTU	The maximum transmission unit specified for the remote device client interface.
Remote interface description	The interface on the remote device that has been enabled to send and receive Layer 2 packets.
Packet totals (in/out)	The total number of packets forwarded in each direction.
byte totals (in/out)	The total number of bytes forwarded in each direction.

Related Commands

Command	Description
mpls l2transport route	Enables routing Layer 2 packets over a specified point-to-point VC by using EoMPLS.

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 [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

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 inter-operability 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
	mvr (global configuration)	Enables and configures multicast VLAN registration on the switch.
	mvr (interface configuration)	Configures MVR ports.
	show mvr interface	Displays the configured MVR interfaces, status of the specified interface, or all multicast groups to which the interface belongs when the interface and members keywords are appended to the command.
	show mvr members	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]]] [ | {begin | exclude | include} expression ]
```

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).
	members	(Optional) Display all MVR groups to which the specified interface belongs.
	vlan <i>vlan-id</i>	(Optional) Display all MVR group members on this VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.
	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.
	12.2(35)SE	The Mode and VLAN fields were added to the output display.

Usage Guidelines

If you enter only the **show mvr interface** command, the output shows all MVR-enabled ports on the switch.

If you enter the **show mvr interface** *interface-id* 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.

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

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

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

```
Switch# show mvr interface fastethernet1/0/6 members
239.255.0.0    DYNAMIC ACTIVE
239.255.0.1    DYNAMIC ACTIVE
239.255.0.2    DYNAMIC ACTIVE
239.255.0.3    DYNAMIC ACTIVE
239.255.0.4    DYNAMIC ACTIVE
239.255.0.5    DYNAMIC ACTIVE
239.255.0.6    DYNAMIC ACTIVE
239.255.0.7    DYNAMIC ACTIVE
239.255.0.8    DYNAMIC ACTIVE
239.255.0.9    DYNAMIC ACTIVE
```

Related Commands

Command	Description
mvr (global configuration)	Enables and configures multicast VLAN registration on the switch.
mvr (interface configuration)	Configures MVR ports.
show mvr	Displays the global MVR configuration on the switch.
show mvr members	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*] [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description

<i>ip-address</i>	(Optional) The IP multicast address. If the address is entered, all receiver and source ports that are members of the multicast group are displayed. 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.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.
12.2(25)SEF	The VLAN and Membership fields were added to the output display.

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.

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

Examples

This is an example of output from the **show 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>

239.255.0.255  INACTIVE  None
239.255.1.0    INACTIVE  None
```

This is an example of output from the **show mvr members ip-address** 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
Switch# show mvr members 239.255.0.2
239.255.0.2      ACTIVE      Fa1/0/1(d), Fa1/0/2(d), Fa1/0/3(d)
                                   Fa1/0/4(d), Fa1/0/5(s)
```

Related Commands

Command	Description
mvr (global configuration)	Enables and configures multicast VLAN registration on the switch.
mvr (interface configuration)	Configures MVR ports.
show mvr	Displays the global MVR configuration on the switch.
show mvr interface	Displays the configured MVR interfaces, status of the specified interface, or all multicast groups to which the interface belongs when the members 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 } [ | { begin | exclude | include } expression ]
```

Syntax Description	
<i>channel-group-number</i>	(Optional) Number of the channel group. The range is 1 to 12.
counters	Display traffic information.
internal	Display internal information.
neighbor	Display neighbor information.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	You can enter any show pagp command to display the active channel-group information. To display the nonactive information, enter the show pagp command with a channel-group number. Expressions are case sensitive. For example, if you enter exclude output, the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

Examples	This is an example of output from the show pagp 1 counters command:

```
Switch> show pagp 1 counters
      Information      Flush      PAgP
Port   Sent   Recv   Sent   Recv   Err Pkts
-----
Channel group: 1
Gi1/0/1   0     0       0     0       0
Gi1/0/1   0     0       0     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
Gi1/0/1	SC	U6/S7	H	30s	1	128	Any	16
Gi1/0/2	SC	U6/S7	H	30s	1	128	Any	16

This is an example of output from the **show pagp 1 neighbor** command:

```
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	Flags	Partner Group Cap.
Gi1/0/1	switch-p2	0002.4b29.4600	Gi1/0/1	9s	SC	10001
Gi1/0/2	switch-p2	0002.4b29.4600	Gi1/0/2	24s	SC	10001

Related Commands

Command	Description
clear pagp	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*}] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

brief	(Optional) Display the name of each macro.
description [<i>interface interface-id</i>]	(Optional) Display all macro descriptions or the description of a specific interface.
name <i>macro-name</i>	(Optional) Display information about a single macro identified by the macro name.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(25)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is a partial output example from the **show parser macro** command. The output for the Cisco-default macros varies depending on the switch platform and the software image running on the switch:

```
Switch# show parser macro
Total number of macros = 6
-----
Macro name : cisco-global
Macro type : default global
# Enable dynamic port error recovery for link state
# failures
errdisable recovery cause link-flap
errdisable recovery interval 60

<output truncated>

-----
Macro name : cisco-desktop
Macro type : default interface
# macro keywords $AVID
# Basic interface - Enable data VLAN only
```

```
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access
```

<output truncated>

```
-----
Macro name : cisco-phone
Macro type : default interface
# Cisco IP phone + desktop template
# macro keywords $AVID $VVID
# VoIP enabled interface - Enable data VLAN
# and voice VLAN (VVID)
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access
```

<output truncated>

```
-----
Macro name : cisco-switch
Macro type : default interface
# macro keywords $NVID
# Access Uplink to Distribution
# Do not apply to EtherChannel/Port Group
# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (NVID) should not be 1
switchport trunk native vlan $NVID
```

<output truncated>

```
-----
Macro name : cisco-router
Macro type : default interface
# macro keywords $NVID
# Access Uplink to Distribution
# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (NVID) should not be 1
switchport trunk native vlan $NVID
```

<output truncated>

```
-----
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
```

This is an example of output from the **show parser macro name** command:

```
Switch# show parser macro name standard-switch10
Macro name : standard-switch10
Macro type : customizable
macro description standard-switch10
# Trust QoS settings on VOIP packets
```

show parser macro

```
auto qos voip trust
# Allow port channels to be automatically formed
channel-protocol pagp
```

This is an example of output from the **show parser macro brief** command:

```
Switch# show parser macro brief
      default global      : cisco-global
      default interface: cisco-desktop
      default interface: cisco-phone
      default interface: cisco-switch
      default interface: cisco-router
      customizable       : snmp
```

This is an example of output from the **show parser macro description** command:

```
Switch# show parser macro description
Global Macro(s): cisco-global
Interface      Macro Description(s)
-----
Fa1/0/1        standard-switch10
Fa1/0/2        this is test macro
-----
```

This is an example of output from the **show parser macro description interface** command:

```
Switch# show parser macro description interface fastethernet1/0/2
Interface      Macro Description
-----
Fa1/0/2        this is test macro
-----
```

Related Commands

Command	Description
macro apply	Applies a macro on an interface or applies and traces a macro on an interface.
macro description	Adds a description about the macros that are applied to an interface.
macro global	Applies a macro on a switch or applies and traces a macro on a switch.
macro global description	Adds a description about the macros that are applied to the switch.
macro name	Creates a macro.
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.

show policy-map

Use the **show policy-map** user EXEC command to display quality of service (QoS) policy maps, which define the traffic policy for a traffic class. Policy maps can include policers that specify the bandwidth limitations and the action to take if the limits are exceeded.

show policy-map [*policy-map-name* [**class** *class-name*] | **interface** *interface-id* [**input** | **output**] [**class** *class-name*]] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description	<i>policy-map-name</i> [class <i>class-name</i>]	(Optional) Display the specified policy map and policy actions for the specified class.
	interface <i>interface-id</i> [input output] [class <i>class-name</i>]	(Optional) For ingress ports, display the policy-map name that is applied to the specified port. For enhanced-services (ES) ports, display the policy-map configuration, Weighted Random Early Detection (WRED) statistics, and policer counters.
		The keywords have these meanings:
		• input—Display the ingress policy-map name applied to the specified port. • output—Display the egress policy-map information applied to the specified ES port. • class <i>class-name</i>—Display statistics for an individual class.
	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples This is an example of output from the **show policy-map** command:

```
Switch> show policy-map

Policy Map pl
  class c1
    Bandwidth 20 (%)
```

show policy-map

```

exponential weight 9
dscp      min-threshold  max-threshold  mark-probability
-----
af11      -              -              1/10
af12      -              -              1/10
af13      -              -              1/10
af21      -              -              1/10
af22      -              -              1/10
af23      -              -              1/10
af31      -              -              1/10
af32      -              -              1/10
af33      -              -              1/10
af41      -              -              1/10
af42      -              -              1/10
af43      -              -              1/10
cs1        -              -              1/10
cs2        -              -              1/10
cs3        -              -              1/10
cs4        -              -              1/10
cs5        -              -              1/10
cs6        -              -              1/10
cs7        -              -              1/10
ef         -              -              1/10
5          1000          6000          1/2000
rsvp       -              -              1/10
default    -              -              1/10
Bandwidth 20 (%)
exponential weight 9
class      min-threshold  max-threshold  mark-probability
-----
0          -              -              1/10
1          -              -              1/10
2          -              -              1/10
3          -              -              1/10
4          -              -              1/10
5          1000          6000          1/2000
6          -              -              1/10
7          -              -              1/10
rsvp       -              -              1/10

```

This is an example of output from the **show policy-map interface *interface-id*** command:

```

Switch> show policy-map interface gigabitethernet1/1/2
GigabitEthernet1/1/2

```

```

service-policy output: vlan-policy

```

```

class-map: vlan10-class (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
match: vlan 10

```

```

Output Queue: Conversation 265
  Bandwidth 80 (%) (800000 kbps) Max Thresh 64 (packets)
Statistics:
  WRED Packets Drop: 0
  WRED Bytes Drop: 0
  Tail Packets Drop: 0
  Tail Bytes Drop: 0

```


Related Commands	Command	Description
	policy-map	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] [ | { begin | exclude | include } expression]
```

Syntax Description

interface <i>interface-id</i>	(Optional) Display port security settings for the specified interface. Valid interfaces include physical ports (including type, module, and port number).
address	(Optional) Display all secure MAC addresses on all ports or a specified port.
vlan	(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 trunk .
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	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 **show port-security address** 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 **show port-security interface interface-id address** 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 **show port-security address interface interface-id vlan** 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**.

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

Examples

This is an example of the output from the **show port-security** command:

```
Switch# show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
              (Count)          (Count)          (Count)
-----
      Gi1/0/1          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 gigabitethernet1/0/1
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    Gi1/0/2      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 interface-id address** command:

```
Switch# show port-security interface gigabitethernet1/0/2 address
Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
      (mins)
-----
      1      0006.0700.0800    SecureConfigured    Gi1/0/2      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 gigabitethernet1/0/2 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
```

 show port-security

Related Commands	Command	Description
	switchport port-security	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 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**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description	<i>segment-id</i>	(Optional) Display REP topology information for the specified segment. The ID range is from 1 to 1024.
	archive	(Optional) Display the previous topology of the segment. This keyword can be useful for troubleshooting a link failure.
	detail	(Optional) Display detailed REP topology information.
	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes User EXEC

Command History	Release	Modification
	12.2(40)SE	This command was introduced.

Usage Guidelines Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples This is 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
```

show rep topology

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
```

Related Commands

Command	Description
rep segment	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 information about the Switch Database Management (SDM) templates that can be used to maximize system resources for a particular feature, or use the command without a keyword to display the template in use.

show sdm prefer [**default** | **routing** | **vlan**] [| {**begin** | **exclude** | **include**} *expression*]



Note

Though visible in the command-line help string, the **dual-ipv4-and-ipv6** keywords are not supported.

Syntax Description

default	(Optional) Display the template that balances system resources among features.
routing	(Optional) Display the template that maximizes system resources for routing.
vlan	(Optional) Display the template that maximizes system resources for Layer 2 VLANs.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.
12.2(25)EY	The routing-pbr keywords were removed.

Usage Guidelines

If you did not reload the switch after entering the **sdm prefer** global configuration command, the **show sdm prefer** privileged EXEC command displays the template in use and not the newly configured template.

The numbers displayed for each template represent an approximate maximum number for each feature resource. The actual number might vary, depending on the actual number of other features configured.

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

Examples

This is an example of output from the **show sdm prefer** command, displaying the template in use:

```
Switch# show sdm prefer
The current template is "desktop default" template.
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.
```

show sdm prefer

```
number of unicast mac addresses:      6K
number of igmp groups + multicast routes: 1K
number of unicast routes:            8K
  number of directly connected hosts:  6K
  number of indirect routes:           2K
number of policy based routing aces:   0
number of qos aces:                   512
number of security aces:              1K
```

This is an example of output from the **show sdm prefer routing** command:

```
Switch# show sdm prefer routing
"desktop 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:      3K
number of igmp groups + multicast routes: 1K
number of unicast routes:            11K
  number of directly connected hosts:  3K
  number of indirect routes:           8K
number of policy based routing aces:   512
number of qos aces:                   512
number of security aces:              1K
```

Related Commands	Command	Description
	sdm prefer	Sets the SDM template to maximize resources for routing, policy-based routing, or VLANs, or to the default template.

show setup express

Use the **show setup express** privileged EXEC command to display if Express Setup mode is active on the switch.

show setup express [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Defaults	No default is defined.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Examples	This is an example of output from the show setup express command:

```
Switch# show setup express
express setup mode is active
```

Related Commands	Command	Description
	setup express	Enables Express Setup mode.

show spanning-tree

Use the **show spanning-tree** user EXEC command to display spanning-tree state information.

```
show spanning-tree [bridge-group | active [detail] | backbonefast | blockedports | bridge | detail
[active] | inconsistentports | interface interface-id | mst | pathcost method | root | summary
[totals] | uplinkfast | vlan vlan-id] [ | { begin | exclude | include } expression]
```

```
show spanning-tree bridge-group [active [detail] | blockedports | bridge | detail [active] |
inconsistentports | interface interface-id | root | summary] [ | { begin | exclude | include }
expression]
```

```
show spanning-tree vlan vlan-id [active [detail] | blockedports | bridge | detail [active] |
inconsistentports | interface interface-id | root | summary] [ | { begin | exclude | include }
expression]
```

```
show spanning-tree { vlan vlan-id | bridge-group } bridge [address | detail | forward-time |
hello-time | id | max-age | priority [system-id] | protocol] [ | { begin | exclude | include }
expression]
```

```
show spanning-tree { vlan vlan-id | bridge-group } root [address | cost | detail | forward-time |
hello-time | id | max-age | port | priority [system-id] [ | { begin | exclude | include }
expression]
```

```
show spanning-tree interface interface-id [active [detail] | cost | detail [active] | inconsistency |
portfast | priority | rootcost | state] [ | { begin | exclude | include } expression]
```

```
show spanning-tree mst [configuration [digest]] [ instance-id [detail | interface interface-id
[detail]] [ | { begin | exclude | include } expression]
```

Syntax Description

<i>bridge-group</i>	(Optional) Specify the bridge group number. The range is 1 to 255.
active [detail]	(Optional) Display spanning-tree information only on active interfaces (available only in privileged EXEC mode).
backbonefast	(Optional) Display spanning-tree BackboneFast status.
blockedports	(Optional) Display blocked port information (available only in privileged EXEC mode).
bridge [address detail forward-time hello-time id max-age priority [system-id] protocol]	(Optional) Display status and configuration of this switch (optional keywords available only in privileged EXEC mode).
detail [active]	(Optional) Display a detailed summary of interface information (active keyword available only in privileged EXEC mode).
inconsistentports	(Optional) Display inconsistent port information (available only in privileged EXEC mode).
interface <i>interface-id</i> [active [detail] cost detail [active] inconsistency portfast priority rootcost state]	(Optional) Display spanning-tree information for the specified interface (all options except portfast and state available only in privileged EXEC mode). Enter each interface separated by a space. Ranges are not supported. Valid interfaces include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 12.

mst [configuration [digest]] [<i>instance-id</i> [detail interface <i>interface-id</i> [detail]]]	(Optional) Display the multiple spanning-tree (MST) region configuration and status (available only in privileged EXEC mode). The keywords have these meanings: • digest—(Optional) Display the MD5 digest included in the current MST configuration identifier (MSTCI). Two separate digests, one for standard and one for prestandard switches, appear (available only in privileged EXEC mode). The terminology was updated for the implementation of the IEEE standard, and the <i>txholdcount</i> field was added. The new master role appears for boundary ports. The word <i>pre-standard</i> or <i>Pre-STD</i> appears when an IEEE standard bridge sends prestandard BPDUs on a port. The word <i>pre-standard (config)</i> or <i>Pre-STD-Cf</i> appears when a port has been configured to transmit prestandard BPDUs and no prestandard BPDU has been received on that port. The word <i>pre-standard (rcvd)</i> or <i>Pre-STD-Rx</i> appears when a prestandard BPDU has been received on a port that has not been configured to transmit prestandard BPDUs. 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. • <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. • interface <i>interface-id</i>—(Optional) Valid interfaces include physical interfaces, VLANs, and NNI port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 48. • detail—(Optional) Display detailed information for the instance or interface.
pathcost method	(Optional) Display the default path cost method (available only in privileged EXEC mode).
root [address cost detail forward-time hello-time id max-age port priority [system-id]]	(Optional) Display root switch status and configuration (all keywords available only in privileged EXEC mode).
summary [totals]	(Optional) Display a summary of interface states or the total lines of the spanning-tree state section.
uplinkfast	(Optional) Display spanning-tree UplinkFast status.
vlan <i>vlan-id</i> [active [detail] backbonefast blockedports bridge [address detail forward-time hello-time id max-age priority [system-id] protocol]	(Optional) Display spanning-tree information for the specified VLAN (some keywords available only in privileged EXEC mode). You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.

show spanning-tree

 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC; indicated keywords available only in privileged EXEC mode.

Command History

Release	Modification
12.1(14)AX	This command was introduced.
12.2(25)SEG	The digest keyword was added, and new digest and transmit hold count fields appear.

Usage Guidelines

If the *vlan-id* variable is omitted, the command applies to the spanning-tree instance for all VLANs.

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

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 (GigabitEthernet1/0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    49153 (priority 49152 sys-id-ext 1)
             Address     0003.fd63.9580
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time   300
  Uplinkfast  enabled

Interface      Role Sts Cost      Prio.Nbr Type
-----
Gi1/0/1        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 (GigabitEthernet1/0/1), cost of root path is 3038
  Topology change flag not set, detected flag not set
  Number of topology changes 0 last change occurred 1d16h ago
  Times: hold 1, topology change 35, notification 2
         hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300
  Uplinkfast enabled

Port 1 (GigabitEthernet1/0/1) of VLAN0001 is forwarding
  Port path cost 3019, Port priority 128, Port Identifier 128.24.
  Designated root has priority 32768, address 0001.42e2.cdd0
  Designated bridge has priority 32768, address 00d0.bbf5.c680
  Designated port id is 128.25, designated path cost 19
  Timers: message age 2, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  Link type is point-to-point by default
  BPDU: sent 0, received 72364
<output truncated>
```

This is an example of output from the **show spanning-tree interface interface-id** command:

```
Switch# show spanning-tree interface gigabitethernet1/0/1
Vlan          Role Sts Cost      Prio.Nbr Type
-----
VLAN0001      Root FWD 3019      128.24  P2p

Switch# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
EtherChannel misconfiguration guard is enabled
Extended system ID is enabled
Portfast is disabled by default
PortFast BPDU Guard is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard is disabled by default
UplinkFast is enabled
BackboneFast is enabled
Pathcost method used is short

Name          Blocking Listening Learning Forwarding STP Active
-----
VLAN0001      1          0          0          11          12
VLAN0002      3          0          0          1          4
VLAN0004      3          0          0          1          4
VLAN0006      3          0          0          1          4
VLAN0031      3          0          0          1          4
VLAN0032      3          0          0          1          4
<output truncated>

-----
37 vlans          109          0          0          47          156
Station update rate set to 150 packets/sec.

UplinkFast statistics
-----
Number of transitions via uplinkFast (all VLANs) : 0
Number of proxy multicast addresses transmitted (all VLANs) : 0
```

show spanning-tree

```
BackboneFast statistics
-----
Number of transition via backboneFast (all VLANs)      : 0
Number of inferior BPDUs received (all VLANs)         : 0
Number of RLQ request PDUs received (all VLANs)       : 0
Number of RLQ response PDUs received (all VLANs)      : 0
Number of RLQ request PDUs sent (all VLANs)           : 0
Number of RLQ response PDUs sent (all VLANs)          : 0
```

This is an example of output from the **show spanning-tree mst configuration** command:

```
Switch# show spanning-tree mst configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
-----
0         1-9,21-4094
1         10-20
-----
```

This is an example of output from the **show spanning-tree mst interface interface-id** command:

```
Switch# show spanning-tree mst interface gigabitEthernet1/0/1
GigabitEthernet1/0/1 of MST00 is root forwarding
Edge port: no (default) port guard : none (default)
Link type: point-to-point (auto) bpdu filter: disable (default)
Boundary : boundary (STP) bpdu guard : disable (default)
Bpdus sent 5, received 74

Instance role state cost prio vlans mapped
0 root FWD 200000 128 1,12,14-4094
```

This is an example of output from the **show spanning-tree 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 Gi1/0/1 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
-----
GigabitEthernet1/0/2 desg FWD 200000 128 P2P bound(STP)
Port-channel1 desg FWD 200000 128 P2P bound(STP)
```

Related Commands

Command	Description
clear spanning-tree counters	Clears the spanning-tree counters.
clear spanning-tree detected-protocols	Restarts the protocol migration process.
spanning-tree backbonefast	Enables the BackboneFast feature.
spanning-tree bpdufilter	Prevents an interface from sending or receiving bridge protocol data units (BPDUs).
spanning-tree bpduguard	Puts an interface in the error-disabled state when it receives a BPDU.
spanning-tree cost	Sets the path cost for spanning-tree calculations.
spanning-tree extend system-id	Enables the extended system ID feature.

Command	Description
spanning-tree guard	Enables the root guard or the loop guard feature for all the VLANs associated with the selected interface.
spanning-tree link-type	Overrides the default link-type setting for rapid spanning-tree transitions to the forwarding state.
spanning-tree loopguard default	Prevents alternate or root ports from becoming the designated port because of a failure that leads to a unidirectional link.
spanning-tree mst configuration	Enters multiple spanning-tree (MST) configuration mode through which the MST region configuration occurs.
spanning-tree mst cost	Sets the path cost for MST calculations.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
spanning-tree mst max-hops	Sets the number of hops in an MST region before the BPDU is discarded and the information held for an interface is aged.
spanning-tree mst port-priority	Configures an interface priority.
spanning-tree mst priority	Configures the switch priority for the specified spanning-tree instance.
spanning-tree mst root	Configures the MST root switch priority and timers based on the network diameter.
spanning-tree mst port-priority	Configures an interface priority.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled interfaces or enables the Port Fast feature on all nontrunking interfaces.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface and all its associated VLANs.
spanning-tree uplinkfast	Accelerates the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself.
spanning-tree vlan	Configures spanning tree on a per-VLAN basis.

show 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**] [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description

<i>interface-id</i>	(Optional) Interface ID for the physical port (including type, module, and port number).
broadcast	(Optional) Display broadcast storm threshold setting.
multicast	(Optional) Display multicast storm threshold setting.
unicast	(Optional) Display unicast storm threshold setting.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

When you enter an *interface-id*, the storm control thresholds are displayed for the specified interface. If you do not enter an *interface-id*, settings are displayed for one traffic type for all ports on the switch. If you do not enter a traffic type, settings are displayed for broadcast storm control. Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of 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
-----
Gi1/0/1    Forwarding    20 pps     10 pps     5 pps
Gi1/0/2    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 1/0/1
Interface      Filter State  Upper      Lower      Current
-----
Gi1/0/1        Forwarding    20 pps     10 pps     5 pps
```

Table 2-28 describes the fields in the **show storm-control** display.

Table 2-28 *show storm-control Field Descriptions*

Field	Description
Interface	Displays the ID of the interface.
Filter State	Displays the status of the filter: - Blocking—Storm control is enabled, and a storm has occurred. - Forwarding—Storm control is enabled, and no storms have occurred. - Inactive—Storm control is disabled.
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
switchport	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 [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	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 10/100 ports; the system jumbo MTU refers to Gigabit ports.
	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

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 1500 bytes
Routing MTU size is 1550 bytes.
```

Related Commands	Command	Description
	system mtu	Sets the MTU size for the Fast Ethernet or Gigabit Ethernet ports.

show udld

Use the **show udld** user EXEC command to display UniDirectional Link Detection (UDLD) administrative and operational status for all interfaces or the specified interface.

show udld [*interface-id*] [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description	<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.
	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	If you do not enter an <i>interface-id</i> , administrative and operational UDLD status for all interfaces are displayed.
	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

Examples	This is an example of output from the show udld interface-id command. For this display, UDLD is enabled on both ends of the link, and UDLD detects that the link is bidirectional. Table 2-29 describes the fields in this display.

```
Switch> show udld fastethernet1/0/11
Interface fa1/0/11
---
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: Fa1/0/12
    Neighbor echo 1 device: Switch-B
    Neighbor echo 1 port: Fa1/0/11
    Message interval: 5
    CDP Device name: Switch-A
```

Table 2-29 *show udd 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 are displayed.
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).

This is an example of output from the **show uddl interface-id** command when the aggressive mode is configured:

```
Switch# show uddl gigabitethernet1/0/1
Interface Gi1/0/1
---
Port enable administrative configuration setting:Enabled / in aggressive mode
Port enable operational state:Enabled / in aggressive mode
Current bidirectional state:Unknown
Current operational state:Link down
Message interval:7
Time out interval:5
No neighbor cache information stored
```

Related Commands

Command	Description
uddl (global configuration)	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
uddl (interface configuration)	Enables UDLD on an individual interface or prevents a fiber-optic port from being enabled by the uddl global configuration command.
uddl reset	Resets all interfaces shut down 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 [ | { begin | exclude | include } expression]
```

Syntax Description	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

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 Internetwork Operating System Software
IOS (tm) C3750ME Software (C3750ME-I5-M), Version 12.2(0.0.35)AX, CISCO DEVELOPMENT
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Mon 13-Oct-03 13:45 by yenanh
Image text-base: 0x00003000, data-base: 0x00A7C3F8

ROM: Bootstrap program is C3750 boot loader
BOOTLDR: C3750ME Boot Loader (C3750ME-HBOOT-M), Version 12.2 [jharrod-congo 100]

SwitchA uptime is 18 hours, 3 minutes
System returned to ROM by power-on
System image file is "flash:c3750me-i5-mz"
```

```
cisco 3750me-24-2-2 (PowerPC405) processor with 120822K/10240K bytes of memory.  
Last reset from power-on  
Bridging software.  
Target IOS Version 12.2(14)AX  
1 Virtual Ethernet/IEEE 802.3 interface(s)  
24 FastEthernet/IEEE 802.3 interface(s)  
4 Gigabit Ethernet/IEEE 802.3 interface(s)  
The password-recovery mechanism is enabled.  
<output truncated>  
1024K bytes of flash-simulated non-volatile configuration memory.
```

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 [**brief** | **dot1q tag native** | **id** *vlan-id* | **internal usage** | **mapping** | **name** *vlan-name* | **private-vlan** [**type**] | **remote-span** | **summary**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax	Description
brief	(Optional) Display one line for each VLAN with the VLAN name, status, and its ports.
dot1q tag native	(Optional) Display the 802.1Q native VLAN tagging status.
id <i>vlan-id</i>	(Optional) Display information about a single VLAN identified by VLAN ID number. For <i>vlan-id</i> , the range is 1 to 4094.
internal usage	(Optional) Display 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 vlan global configuration command until you remove them from internal use.
mapping	(Optional) Display VLAN mapping information (contents of the VLAN mapping table) for the enhanced-services (ES) ports. This command is supported only in privileged EXEC mode.
name <i>vlan-name</i>	(Optional) Display information about a single VLAN identified by VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.
private-vlan	(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. This keyword is only supported if your switch is running the EMI.
type	(Optional) Display only private VLAN ID and type.
remote-span	(Optional) Display information about Remote SPAN (RSPAN) VLANs.
summary	(Optional) Display VLAN summary information.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.



Note

Though visible in the command-line help string, the **ifindex** and **private-vlan** keywords are not supported.

Command Modes

User EXEC, Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.
12.2(25)EY	The private-vlan keyword was added.

Usage Guidelines

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 type displayed as *normal* means a VLAN that 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 without removing 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*.

Expressions are case sensitive. For example, if you enter **exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show vlan** command. [Table 2-30](#) describes each field in the display.

```
Switch> show vlan
VLAN Name                Status      Ports
-----
1    default                active      Fa1/0/1, Fa1/0/3, Fa1/0/4
                                           Fa1/0/5, Fa1/0/6, Fa1/0/7
                                           Fa1/0/8, Fa1/0/9, Fa1/0/10
                                           Fa1/0/11, Fa1/0/12, Fa1/0/13
                                           Fa1/0/14, Fa1/0/15, Fa1/0/16
                                           Fa1/0/17, Fa1/0/18, Fa1/0/19
                                           Fa1/0/20, Fa1/0/21, Fa1/0/22
                                           Fa1/0/23, Fa1/0/24, Gi1/0/1
                                           Gi1/0/2, Gi1/1/1, Gi1/1/2
30   VLAN0030                active      Fa1/0/2
50   VLAN0050                active
200  VLAN0200                active
300  VLAN0300                active
400  VLAN0400                active
1002 fddi-default           act/unsup
1003 token-ring-default     act/unsup
1004 fddinet-default        act/unsup
1005 trnet-default          act/unsup

VLAN Type  SAID          MTU    Parent RingNo BridgeNo Stp    BrdgMode Trans1 Trans2
-----
1    enet  100001       1500   -      -      -      -    -      0      0
30   enet  100030       1500   -      -      -      -    -      0      0
50   enet  100050       1500   -      -      -      -    -      0      0
200  enet  100200       1500   -      -      -      -    -      0      0
300  enet  100300       1500   -      -      -      -    -      0      0
400  enet  100400       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

Remote SPAN VLANs
-----
```

Primary Secondary Type Ports

Table 2-30 *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	Not applicable to this release.

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

```
Switch> show vlan summary
Number of existing VLANs      : 45
Number of existing VTP VLANs  : 45
Number of existing extended VLANs : 0
```

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

```
Switch# show vlan id 2
VLAN Name                Status    Ports
-----
2    VLAN0200                active    Fa1/0/17, Fa1/0/18, Fa1/0/21
                                   Gi1/0/1

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 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 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.

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      Gi3/0/3
10      502      community     Fa2/0/11
10      503      non-operational3 -
20      25       isolated      Fa1/0/13, Fa1/0/20, Fa1/0/22, Gi1/0/1, Fa2/0/13,
Fa2/0/22, Fa3/0/13, Fa3/0/14, Fa3/0/20, Gi3/0/1
20      30       community     Fa1/0/13, Fa1/0/20, Fa1/0/21, Gi1/0/1, Fa2/0/13,
Fa2/0/20, Fa3/0/14, Fa3/0/20, Fa3/0/21, Gi3/0/1
20      35       community     Fa1/0/13, Fa1/0/20, Fa1/0/23, Fa1/0/33. Gi1/0/1,
Fa2/0/13, Fa3/0/14, Fa3/0/20. Fa3/0/23, Fa3/0/33,
Gi3/0/1
20      55       non-operational
2000    2500     isolated      Fa1/0/5, Fa1/0/10, Fa2/0/5, Fa2/0/10, Fa2/0/15
```

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
```

```
Switch> show vlan internal usage
VLAN Usage
-----
1025 FastEthernet1/0/23
1026 FastEthernet1/0/24
```

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

```
Switch# show vlan mapping
Interface Gi1/1/1:
  Outer VLAN   Inner VLAN   Translated VLAN
  -----
      10        20        120
      10         -        drop
      10        21        121
      11        30        130
      11        31        131
      50         -         60
      51         -         61
Interface Gi1/1/2:
  Outer VLAN   Inner VLAN   Translated VLAN
  -----
      11         -        drop
      11        30        130
      11        31        131
      80         -        800
      90         -        900
```

Related Commands	Command	Description
	private-vlan	Configures a VLAN as a community, isolated, or primary VLAN or associates a primary VLAN with secondary VLANs.
	switchport mode	Configures the VLAN membership mode of a port.
	vlan (global configuration)	Enables config-vlan mode where you can configure VLANs 1 to 4094.
	vlan (VLAN configuration)	Configures VLAN characteristics in the VLAN database. Only available for normal-range VLANs (VLAN IDs 1 to 1005). Do not enter leading zeros.

show vlan access-map

Use the **show vlan access-map** privileged EXEC command to display information about a particular VLAN access map or all VLAN access maps.

show vlan access-map [*mapname*] [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description	<i>mapname</i>	(Optional) Name of a specific VLAN access map.
	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

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
```

Related Commands	Command	Description
	show vlan filter	Displays information about all VLAN filters or about a particular VLAN or VLAN access map.
	vlan access-map	Creates a VLAN map entry for VLAN packet filtering.
	vlan filter	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*] [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description

access-map <i>name</i>	(Optional) Display filtering information for the specified VLAN access map.
vlan <i>vlan-id</i>	(Optional) Display filtering information for the specified VLAN. The range is 1 to 4094.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

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

Examples

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

```
Switch# show vlan filter
VLAN Map map_1 is filtering VLANs:
  20-22
```

Related Commands

Command	Description
show vlan access-map	Displays information about a particular VLAN access map or all VLAN access maps.
vlan access-map	Creates a VLAN map entry for VLAN packet filtering.
vlan filter	Applies a VLAN map to one or more VLANs.

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**] [**|** { **begin** | **exclude** | **include** } *expression*]

Syntax Description	statistics	(Optional) Display VQP client-side statistics and counters.
	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	User EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

Examples	This is an example of output from the show vmps command:

```
Switch> show vmps
VQP Client Status:
-----
VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server:

Reconfirmation status
-----
VMPS Action:          other
```

This is an example of output from the **show vmps statistics** command. [Table 2-31](#) describes each field in the display.

```
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 2-31 *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.
VQP Wrong Domain	Number of times the management domain in the request does not match the one for the VMPS. Any previous VLAN assignments of the port are not changed. This response means that the server and the client have not been configured with the same VTP management domain.
VQP Wrong Version	Number of times the version field in the query packet contains a value that is higher than the version supported by the VMPS. The VLAN assignment of the port is not changed. The switches send only VMPS version 1 requests.
VQP Insufficient Resource	Number of times the VMPS is unable to answer the request because of a resource availability problem. If the retry limit has not yet been reached, the client repeats the request with the same server or with the next alternate server, depending on whether the per-server retry count has been reached.

Related Commands	Command	Description
	clear vmps statistics	Clears the statistics maintained by the VQP client.
	vmps reconfirm (privileged EXEC)	Sends VQP queries to reconfirm all dynamic VLAN assignments with the VMPS.
	vmps retry	Configures the per-server retry count for the VQP client.
	vmps server	Configures the primary VMPS and up to three secondary servers.

show vtp

Use the **show vtp** user EXEC command to display general information about the VLAN Trunking Protocol (VTP) management domain, status, and counters.

show vtp {counters | status} [| {begin | exclude | include} *expression*]

Syntax Description

counters	Display the VTP statistics for the switch.
status	Display general information about the VTP management domain status.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show vtp counters** command. [Table 2-32](#) describes each field in the display.

```
Switch> show vtp counters
```

VTP statistics:

```
Summary advertisements received      : 0
Subset advertisements received       : 0
Request advertisements received      : 0
Summary advertisements transmitted   : 0
Subset advertisements transmitted    : 0
Request advertisements transmitted    : 0
Number of config revision errors     : 0
Number of config digest errors       : 0
Number of V1 summary errors          : 0
```

VTP pruning statistics:

Trunk	Join Transmitted	Join Received	Summary advts received from non-pruning-capable device
-----	-----	-----	-----
Fa1/0/17	0	0	0
Fa1/0/18	0	0	0

Table 2-32 *show vtp counters Field Descriptions*

Field	Description
Summary advertisements received	Number of summary advertisements received by this switch on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update timestamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements received	Number of subset advertisements received by this switch on its trunk ports. Subset advertisements contain all the information for one or more VLANs.
Request advertisements received	Number of advertisement requests received by this switch on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
Summary advertisements transmitted	Number of summary advertisements sent by this switch on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update timestamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements transmitted	Number of subset advertisements sent by this switch on its trunk ports. Subset advertisements contain all the information for one or more VLANs.
Request advertisements transmitted	Number of advertisement requests sent by this switch on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
Number of configuration revision errors	Number of revision errors. Whenever you define a new VLAN, delete an existing one, suspend or resume an existing VLAN, or modify the parameters on an existing VLAN, the configuration revision number of the switch increments. Revision errors increment whenever the switch receives an advertisement whose revision number matches the revision number of the switch, but the MD5 digest values do not match. This error means that the VTP password in the two switches is different or that the switches have different configurations. These errors means that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.
Number of configuration digest errors	Number of MD5 digest errors. Digest errors increment whenever the MD5 digest in the summary packet and the MD5 digest of the received advertisement calculated by the switch do not match. This error usually means that the VTP password in the two switches is different. To solve this problem, make sure that the VTP password on all switches is the same. These errors mean that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.

Table 2-32 *show vtp counters Field Descriptions (continued)*

Field	Description
Number of V1 summary errors	Number of version 1 errors. Version 1 summary errors increment whenever a switch in VTP V2 mode receives a VTP version 1 frame. These errors mean that at least one neighboring switch is either running VTP version 1 or VTP version 2 with V2-mode disabled. To solve this problem, change the configuration of the switches in VTP V2-mode to disabled.
Join Transmitted	Number of VTP pruning messages sent on the trunk.
Join Received	Number of VTP pruning messages received on the trunk.
Summary Advts Received from non-pruning-capable device	Number of VTP summary messages received on the trunk from devices that do not support pruning.

This is an example of output from the **show vtp status** command. [Table 2-33](#) describes each field in the display.

```
Switch> show vtp status
VTP Version                : 2
Configuration Revision     : 39
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 10
VTP Operating Mode         : Server
VTP Domain Name            :
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                 : 0x77 0x26 0x9F 0x96 0x03 0x7D 0xFC 0xB2
Configuration last modified by 10.89.152.146 at 3-1-93 00:04:30
Local updater ID is 10.89.152.146 on interface Vl1 (lowest numbered VLAN interf)
```

Table 2-33 *show vtp status Field Descriptions*

Field	Description
VTP Version	Displays the VTP version operating on the switch. By default, the switch implements version 1 but can be set to version 2.
Configuration Revision	Current configuration revision number on this switch.
Maximum VLANs Supported Locally	Maximum number of VLANs supported locally.
Number of Existing VLANs	Number of existing VLANs.

Table 2-33 *show vtp status Field Descriptions (continued)*

Field	Description
VTP Operating Mode	Displays the VTP operating mode, which can be server, client, or transparent. Server: a switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The switch guarantees that it can recover all the VLAN information in the current VTP database from NVRAM after reboot. By default, every switch is a VTP server. Note The switch automatically changes from VTP server mode to VTP client mode if it detects a failure while writing the configuration to NVRAM and cannot return to server mode until the NVRAM is functioning. Client: a switch in VTP client mode is enabled for VTP, can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on it. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database. Transparent: a switch in VTP transparent mode is disabled for VTP, does not send or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The switch receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received.
VTP Domain Name	Name that identifies the administrative domain for the switch.
VTP Pruning Mode	Displays whether pruning is enabled or disabled. Enabling pruning on a VTP server enables pruning for the entire management domain. Pruning restricts flooded traffic to those trunk links that the traffic must use to access the appropriate network devices.
VTP V2 Mode	Displays if VTP version 2 mode is enabled. All VTP version 2 switches operate in version 1 mode by default. Each VTP switch automatically detects the capabilities of all the other VTP devices. A network of VTP devices should be configured to version 2 only if all VTP switches in the network can operate in version 2 mode.
VTP Traps Generation	Displays whether VTP traps are sent to a network management station.
MD5 Digest	A 16-byte checksum of the VTP configuration.
Configuration Last Modified	Displays the date and time of the last configuration modification. Displays the IP address of the switch that caused the configuration change to the database.

 show vtp

Related Commands	Command	Description
	clear vtp counters	Clears the VTP and pruning counters.
	vtp (global configuration)	Configures the VTP filename, interface name, domain name, and mode.
	vtp (VLAN configuration)	Configures the VTP domain name, password, pruning, and mode.

shutdown

Use the **shutdown** interface configuration command to disable an interface. Use the **no** form of this command to restart a disabled interface.

shutdown

no shutdown

Syntax Description	This command has no arguments or keywords.

Defaults	The interface is enabled by default.

Command Modes	Interface configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	The shutdown command for a port causes it to stop forwarding. You can enable the port with the no shutdown command.
	The no shutdown command has no effect if the port is a static-access port assigned to a VLAN that has been deleted, suspended, or shut down. The port must first be a member of an active VLAN before it can be re-enabled.
	The shutdown command disables all functions on the specified interface.
	This command also marks the interface as unavailable. To see if an interface is disabled, use the show interfaces privileged EXEC command. An interface that has been shut down is shown as administratively down in the display.

Examples	These examples show how to disable and re-enable a port:

```
Switch(config)# interface gigabitethernet1/0/2  
Switch(config-if)# shutdown
```

```
Switch(config)# interface gigabitethernet1/0/2  
Switch(config-if)# no shutdown
```

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

Related Commands	Command	Description
	show interfaces	Displays the statistical information specific to all interfaces or to a specific interface.

shutdown vlan

Use the **shutdown vlan** global configuration command to shut down (suspend) local traffic on the specified VLAN. Use the **no** form of this command to restart local traffic on the VLAN.

shutdown vlan *vlan-id*

no shutdown vlan *vlan-id*

Syntax Description	<i>vlan-id</i> ID of the VLAN to be locally shut down. The range is 2 to 1001. VLANs defined as default VLANs under the VLAN Trunking Protocol (VTP), as well as extended-range VLANs (greater than 1005) cannot be shut down. The default VLANs are 1 and 1002 to 1005.							
Defaults	No default is defined.							
Command Modes	Global configuration							
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.1(14)AX</td><td>This command was introduced.</td></tr></table>		Release	Modification	12.1(14)AX	This command was introduced.		
Release	Modification							
12.1(14)AX	This command was introduced.							
Usage Guidelines	The shutdown vlan command does not change the VLAN information in the VTP database. It shuts down traffic locally, but the switch still advertises VTP information.							
Examples	This example shows how to shutdown traffic on VLAN 2: <pre>Switch(config)# shutdown vlan 2</pre> You can verify your setting by entering the show vlan privileged EXEC command.							
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>shutdown (config-vlan mode)</td><td>Shuts down local traffic on the VLAN when in config-VLAN mode (accessed by the vlan <i>vlan-id</i> global configuration command).</td></tr><tr><td>vlan database</td><td>Enters VLAN configuration mode.</td></tr></table>		Command	Description	shutdown (config-vlan mode)	Shuts down local traffic on the VLAN when in config-VLAN mode (accessed by the vlan <i>vlan-id</i> global configuration command).	vlan database	Enters VLAN configuration mode.
Command	Description							
shutdown (config-vlan mode)	Shuts down local traffic on the VLAN when in config-VLAN mode (accessed by the vlan <i>vlan-id</i> global configuration command).							
vlan database	Enters VLAN configuration mode.							

small-frame violation rate

Use the **small-frame violation rate** *pps* interface configuration command on the switch stack or on a standalone switch to configure the rate (threshold) for an interface to be error disabled when it receives VLAN-tagged packets that are small frames (67 bytes or less) at the specified rate. Use the **no** form of this command to return to the default setting.

small-frame violation rate *pps*

no small-frame violation rate *pps*

Syntax Description	pps	Specify the threshold at which an interface receiving small frames will be error disabled. The range is 1 to 10,000 packets per second (pps).

Defaults	This feature is disabled.

Command Modes	Interface configuration

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

Usage Guidelines	This command enables the rate (threshold) for a port to be error disabled when it receives small frames. Small frames are considered packets that are 67 frames or less.
	Use the errdisable detect cause small-frame global configuration command to globally enable the small-frames threshold for each port.
	You can configure the port to be automatically re-enabled by using the errdisable recovery cause small-frame global configuration command. You configure the recovery time by using the errdisable recovery interval <i>interval</i> <i>global configuration command</i> .

Examples	This example shows how to enable the small-frame arrival rate feature so that the port is error disabled if incoming small frames arrived at 10,000 pps.
	<pre>Switch(config)# interface gigabitethernet2/0/1 Switch(config-if)# small-frame violation rate 10000</pre>
	You can verify your setting by entering the privileged EXEC command.

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

snmp 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

Syntax Description

trap-rate <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).

Defaults

Sending REP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(40)SE	This command was introduced.

Usage Guidelines

Use this command to enable the switch to send REP specific traps corresponding to link operational status changes and port role changes.

Examples

This example configures the switch to send REP traps at a rate of 10 per second:

```
Switch(config)# snmp mib rep trap-rate 10
```

Related Commands

Command	Description
show running config	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 | cluster | config | copy-config | cpu threshold | {dot1x [auth-fail-vlan | guest-vlan | no-auth-fail-vlan | no-guest-vlan] } | entity | envmon [fan | shutdown | supply | temperature] | flash | hsrp | ipmulticast | mac-notification | msdp | ospf [cisco-specific | errors | lsa | rate-limit | retransmit | state-change] | pim [invalid-pim-message | neighbor-change | rp-mapping-change] | mac-notification | port-security [trap-rate *value*] | rtr | rsvp | snmp [authentication | coldstart | linkdown | linkup | warmstart] | storm-control trap-rate *value* | stpx | syslog | tty | vlancreate | vlandelete | vlan-membership | vtp]

no snmp-server enable traps [bgp | bridge | cluster | config | copy-config | cpu threshold | {dot1x [auth-fail-vlan | guest-vlan | no-auth-fail-vlan | no-guest-vlan] } | entity | envmon [fan | shutdown | supply | temperature] | flash | hsrp | ipmulticast | mac-notification | msdp | ospf [cisco-specific | errors | lsa | rate-limit | retransmit | state-change] | pim [invalid-pim-message | neighbor-change | rp-mapping-change] | mac-notification | port-security [trap-rate] | rtr | rsvp | snmp [authentication | coldstart | linkdown | linkup | warmstart] | storm-control trap-rate *value* | stpx | syslog | tty | vlancreate | vlandelete | vlan-membership | vtp]

Syntax Description

bgp	(Optional) Enable Border Gateway Protocol (BGP) state-change traps.
bridge	(Optional) Generate STP bridge MIB traps.
cluster	(Optional) Enable cluster traps.
config	(Optional) Enable SNMP configuration traps.
copy-config	(Optional) Enable SNMP copy configuration traps.
cpu threshold	(Optional) Allow CPU-related traps.
dot1x [auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan]	(Optional) Enable IEEE 802.1x traps. The keywords have these meanings: • auth-fail-vlan—(Optional) Generate a trap when the port moves to the configured restricted VLAN. • guest-vlan—(Optional) Generate a trap when the port moves to the configured guest VLAN. • no-auth-fail-vlan—(Optional) Generate a trap when a port tries to enter the restricted VLAN, but cannot because the restricted VLAN is not configured. • no-guest-vlan—(Optional) Generate a trap when a port tries to enter the guest VLAN, but cannot because the guest VLAN is not configured.
Note	When the snmp-server enable traps dot1x command is entered (without any other keywords specified), all the IEEE 802.1x traps are enabled.
entity	(Optional) Enable SNMP entity traps.
envmon	(Optional) Generate environmental monitor traps.
fan	(Optional) Generate environmental fan trap.

shutdown	(Optional) Generate environmental monitor shutdown traps.
supply	(Optional) Generate environmental monitor power supply traps.
temperature	(Optional) Generate environmental monitor temperature traps.
flash	(Optional) Enable SNMP FLASH notifications.
hsrp	(Optional) Enable Hot Standby Router Protocol (HSRP) traps.
ipmulticast	(Optional) Enable IP multicast routing traps.
mac-notification	(Optional) Enable MAC address notification traps.
mdsp	(Optional) Enable Multicast Source Discovery Protocol (MSDP) traps.
ospf [cisco-specific errors lsa rate-limit retransmit state-change]	(Optional) Enable Open Shortest Path First (OSPF) traps. The keywords have these meanings: • cisco-specific—(Optional) Enable Cisco-specific traps. • errors—(Optional) Enable error traps. • lsa—(Optional) Enable link-state advertisement (LSA) traps. • rate-limit—(Optional) Enable rate-limit traps. • retransmit—(Optional) Enable packet-retransmit traps. • state-change—(Optional) Enable state-change traps.
pim	(Optional) Enable Protocol-Independent Multicast (PIM) traps.
invalid-pim-message	(Optional) Enable invalid PIM message traps.
neighbor-change	(Optional) Enable PIM neighbor-change traps.
rp-mapping-change	(Optional) Enable rendezvous point (RP)-mapping change traps.
mac-notification	(Optional) Enable MAC address notification traps.
port-security	(Optional) Enable SNMP port security traps.
trap-rate <i>value</i>	(Optional) 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 occurrence).
rsvp	(Optional) Enable Resource Reservation Protocol (RSVP) flow change traps.
rtr	(Optional) Enable SNMP Response Time Reporter traps.
snmp	(Optional) Enable SNMP traps.
authentication	(Optional) Enable authentication trap.
coldstart	(Optional) Enable cold start trap.
linkdown	(Optional) Enable linkdown trap.
linkup	(Optional) Enable linkup trap.
warmstart	(Optional) Enable warmstart trap.
storm-control trap-rate <i>value</i>	(Optional) Enable storm-control traps. Use the trap-rate 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 occurrence).
stpx	(Optional) Enable SNMP STPX MIB traps.
syslog	(Optional) Enable SNMP syslog traps.
tty	(Optional) Send TCP connection traps. This is enabled by default.
vlan-membership	(Optional) Enable SNMP VLAN membership traps.
vlancreate	(Optional) Enable SNMP VLAN-created traps.

vlandelete	(Optional) Enable SNMP VLAN-deleted traps.
vtp	(Optional) Enable VLAN Trunking Protocol (VTP) traps.

**Note**

Though visible in the command-line help strings, the **snmp-server enable informs** command is not supported. To enable the sending of SNMP inform notifications, use the **snmp-server enable traps** command combined with the **snmp-server host *host-addr* informs** command. Though visible, the **fru-control**, **flash insertion** and **flash removal** keywords are not supported.

Defaults

The sending of SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.
12.2(25)EY	The ipmulticast , msdp , ospf [cisco-specific errors lsa rate-limit retransmit state-change], pim [invalid-pim-message neighbor-change rp-mapping-change], tty , and storm-control trap-rate keywords were added.
12.2(46)SE	The dot1x [auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan] keywords were added.
12.2(50)SE	The cpu threshold 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.

Use the **snmp-server enable traps** command to enable sending of traps or informs, when supported.

**Note**

Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to send VTP traps to the NMS:

```
Switch(config)# snmp-server enable traps vtp
```

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

Related Commands	Command	Description
	show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.
	snmp-server host	Specifies the host that receives SNMP traps.

snmp-server host

Use the **snmp-server host** global configuration command to specify the recipient (host) of a Simple Network Management Protocol (SNMP) notification operation. Use the **no** form of this command to remove the specified host.

```
snmp-server host host-addr [informs | traps] [version { 1 | 2c | 3 {auth | noauth| priv}}] [vrf
vrf-instance] {community-string [notification-type]}

no snmp-server host host-addr [informs | traps] [version { 1 | 2c | 3 {auth | noauth | priv}}]
community-string
```

Syntax Description	host-addr	Name or Internet address of the host (the targeted recipient).
	informs traps	(Optional) Send SNMP traps or informs to this host.
	version 1 2c 3	(Optional) Version of the Simple Network Management Protocol (SNMP) used to send the traps.
		These keywords are supported:
		1 —SNMPv1. This option is not available with informs. 2c —SNMPv2C. 3 —SNMPv3. These optional keywords can follow the version 3 keyword: • auth (Optional). Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. • noauth (Default). The noAuthNoPriv security level. This is the default if the [auth noauth priv] keyword choice is not specified. • priv (Optional). Enables Data Encryption Standard (DES) packet encryption (also called <i>privacy</i>).
	Note	The priv keyword is available only when the crypto (encrypted) software image is installed.
	vrf vrf-instance	(Optional) Virtual private network (VPN) routing instance and name for this host.

community-string

Password-like community string sent with the notification operation. Though you can set this string by using the **snmp-server host** command, we recommend that you define this string by using the **snmp-server community** global configuration command before using the **snmp-server host** command.

Note The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.

<i>notification-type</i>	(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: • bgp—Send Border Gateway Protocol (BGP) state change traps. This keyword is available only when the enhanced multilayer image is installed on the stack master. • bridge—Send SNMP Spanning Tree Protocol (STP) bridge MIB traps. • cluster—Send cluster member status traps. • config—Send SNMP configuration traps. • copy-config—Send SNMP copy configuration traps. • 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. • stpx—Send SNMP STP extended MIB traps. • syslog—Send SNMP syslog traps. • tty—Send TCP connection traps. • udp-port port—Configure the User Datagram Protocol (UDP) port number of the host to receive the traps. The range is from 0 to 65535. • vlan-membership— Send SNMP VLAN membership traps. • vlancreate—Send SNMP VLAN-created traps. • vlandelete—Send SNMP VLAN-deleted traps. • vtp—Send SNMP VLAN Trunking Protocol (VTP) traps.

**Note**

Though visible in the command-line help strings, the **fru-ctrl** keyword is 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
12.1(14)AX	This command was introduced.
12.2(25)EY	The ipmulticast , msdp , pim , storm-control and vrf vrf-instance keywords were added. The command syntax was changed.
12.2(50)SE	The cpu threshold 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
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.
snmp-server enable traps	Enables SNMP notification for various trap types or inform requests.

snmp trap mac-notification

Use the **snmp trap mac-notification** interface configuration command to enable the Simple Network Management Protocol (SNMP) MAC address notification trap on a specific Layer 2 interface. Use the **no** form of this command to return to the default setting.

snmp trap mac-notification {added | removed}

no snmp trap mac-notification {added | removed}

Syntax Description	added	Enable the MAC notification trap whenever a MAC address is added on this interface.
	removed	Enable the MAC notification trap whenever a MAC address is removed from this interface.

Defaults By default, the traps for both address addition and address removal are disabled.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(14)AX	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 fastethernet1/0/4
Switch(config-if)# snmp trap mac-notification added
```

You can verify your settings by entering the **show mac address-table notification interface** privileged EXEC command.

Related Commands	Command	Description
	clear mac address-table notification	Clears the MAC address notification global counters.
	mac address-table notification	Enables the MAC address notification feature.
	show mac address-table notification	Displays the MAC address notification settings for all interfaces or on the specified interface when the interface keyword is appended.
	snmp-server enable traps	Sends the SNMP MAC notification traps when the mac-notification keyword is appended.

spanning-tree backbonefast

Use the **spanning-tree backbonefast** global configuration command to enable the BackboneFast feature. Use the **no** form of the command to return to the default setting.

spanning-tree backbonefast

no spanning-tree backbonefast

Syntax Description This command has no arguments or keywords.

Defaults BackboneFast is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines You can configure the BackboneFast feature for rapid-PVST+ or for multiple spanning-tree (MST) mode, but the feature remains disabled (inactive) until you change the spanning-tree mode to PVST+.

BackboneFast starts when a root port or blocked port on a switch receives inferior BPDUs from its designated switch. An inferior BPDU identifies a switch that declares itself as both the root bridge and the designated switch. When a switch receives an inferior BPDU, it means that a link to which the switch is not directly connected (an *indirect* link) has failed (that is, the designated switch has lost its connection to the root switch. If there are alternate paths to the root switch, BackboneFast causes the maximum aging time on the ports on which it received the inferior BPDU to expire and allows a blocked port to move immediately to the listening state. BackboneFast then transitions the port to the forwarding state. For more information, see the software configuration guide for this release.

Enable BackboneFast on all supported switches to allow the detection of indirect link failures and to start the spanning-tree reconfiguration sooner.

Examples This example shows how to enable BackboneFast on the switch:

```
Switch(config)# spanning-tree backbonefast
```

You can verify your setting by entering the **show spanning-tree summary** privileged EXEC command.

Related Commands	Command	Description
	show spanning-tree summary	Displays a summary of the spanning-tree port states.

spanning-tree bpdupfilter

Use the **spanning-tree bpdupfilter** interface configuration command to prevent an interface from sending or receiving bridge protocol data units (BPDUs). Use the **no** form of this command to return to the default setting.

spanning-tree bpdupfilter { disable | enable }

no spanning-tree bpdupfilter

Syntax Description

disable	Disable BPDU filtering on the specified interface.
enable	Enable BPDU filtering on the specified interface.

Defaults

BPDU filtering is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

You can enable the BPDU filtering feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode.



Caution

Enabling BPDU filtering on an interface is the same as disabling spanning tree on it and can result in spanning-tree loops.

You can globally enable BPDU filtering on all Port Fast-enabled interfaces by using the **spanning-tree portfast bpdupfilter default** global configuration command.

You can use the **spanning-tree bpdupfilter** interface configuration command to override the setting of the **spanning-tree portfast bpdupfilter default** global configuration command.

Examples

This example shows how to enable BPDU filtering on a port:

```
Switch(config)# interface fastethernet1/0/1
Switch(config-if)# spanning-tree bpdupfilter enable
```

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

Related Commands	Command	Description
	show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.
	spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled interfaces or enables the Port Fast feature on all nontrunking interfaces.
	spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface and all its associated VLANs.

spanning-tree bpduguard

Use the **spanning-tree bpduguard** interface configuration command to put an interface in the error-disabled state when it receives a bridge protocol data unit (BPDU). Use the **no** form of this command to return to the default setting.

spanning-tree bpduguard {disable | enable}

no spanning-tree bpduguard

Syntax Description

disable	Disable BPDU guard on the specified interface.
enable	Enable BPDU guard on the specified interface.

Defaults

BPDU guard is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The BPDU guard feature provides a secure response to invalid configurations because you must manually put the interface back in service. Use the BPDU guard feature in a service-provider network to prevent an interface from being included in the spanning-tree topology.

You can enable the BPDU guard feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode.

You can globally enable BPDU guard on all Port Fast-enabled interfaces by using the **spanning-tree portfast bpduguard default** global configuration command.

You can use the **spanning-tree bpduguard** interface configuration command to override the setting of the **spanning-tree portfast bpduguard default** global configuration command.

Examples

This example shows how to enable the BPDU guard feature on a port:

```
Switch(config)# interface fastethernet1/0/1  
Switch(config-if)# spanning-tree bpduguard enable
```

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

Related Commands	Command	Description
	show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.
	spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled interfaces or enables the Port Fast feature on all nontrunking interfaces.
	spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface and all its associated VLANs.

spanning-tree cost

Use the **spanning-tree cost** interface configuration command to set the path cost for spanning-tree calculations. If a loop occurs, spanning tree considers the path cost when selecting an interface to place in the forwarding state. Use the **no** form of this command to return to the default setting.

spanning-tree [**vlan** *vlan-id*] **cost** *cost*

no spanning-tree [**vlan** *vlan-id*] **cost**

Syntax Description

vlan <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 interface 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
12.1(14)AX	This command was introduced.

Usage Guidelines

When you configure the cost, higher values represent higher costs.

If you configure an interface with both the **spanning-tree vlan** *vlan-id* **cost** *cost* command and the **spanning-tree cost** *cost* command, the **spanning-tree vlan** *vlan-id* **cost** *cost* command takes effect.

Examples

This example shows how to set the path cost to 250 on a port:

```
Switch(config)# interface fastethernet1/0/4
Switch(config-if)# spanning-tree cost 250
```

This example shows how to set a path cost to 300 for VLANs 10, 12 to 15, and 20:

```
Switch(config-if)# spanning-tree vlan 10,12-15,20 cost 300
```

You can verify your settings by entering the **show spanning-tree interface** *interface-id* privileged EXEC command.

Related Commands	Command	Description
	show spanning-tree interface <i>interface-id</i>	Displays spanning-tree information for the specified interface.
	spanning-tree port-priority	Configures an interface priority.
	spanning-tree vlan priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree etherchannel guard misconfig

Use the **spanning-tree etherchannel guard misconfig** global configuration command to display an error message when the switch detects an EtherChannel misconfiguration. Use the **no** form of this command to disable the feature.

spanning-tree etherchannel guard misconfig

no spanning-tree etherchannel guard misconfig

Syntax Description

This command has no arguments or keywords.

Defaults

EtherChannel guard is enabled on the switch.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)EY	This command was introduced.

Usage Guidelines

When the switch detects an EtherChannel misconfiguration, this error message appears:

```
PM-4-ERR_DISABLE: Channel-misconfig error detected on [chars], putting [chars] in err-disable state.
```

To show switch ports that are in the misconfigured EtherChannel, use the **show interfaces status err-disabled** privileged EXEC command. To verify the EtherChannel configuration on a remote device, use the **show etherchannel summary** privileged EXEC command on the remote device.

When a port is in the error-disabled state because of an EtherChannel misconfiguration, you can bring it out of this state by entering the **errdisable recovery cause channel-misconfig** global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shut down** interface configuration commands.

Examples

This example shows how to enable the EtherChannel guard misconfiguration feature:

```
Switch(config)# spanning-tree etherchannel guard misconfig
```

You can verify your settings by entering the **show spanning-tree summary** privileged EXEC command.

Related Commands	Command	Description
	errdisable recovery cause channel-misconfig	Enables the timer to recover from the EtherChannel misconfiguration error-disable state.
	show etherchannel summary	Displays EtherChannel information for a channel as a one-line summary per channel-group.
	show interfaces status err-disabled	Displays the interfaces in the error-disabled state.

spanning-tree extend system-id

Use the **spanning-tree extend system-id** global configuration command to enable the extended system ID feature.

spanning-tree extend system-id



Note

Though visible in the command-line help strings, the **no** version of this command is not supported. You cannot disable the extended system ID feature.

Syntax Description

This command has no arguments or keywords.

Defaults

The extended system ID is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The switch supports the 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 an instance identifier for the multiple spanning tree [MST]).

The spanning tree uses the extended system ID, the switch priority, and the allocated spanning-tree MAC address to make the bridge ID unique for each VLAN or multiple spanning-tree instance.

Support for the extended system ID affects how you manually configure the root switch, the secondary root switch, and the switch priority of a VLAN. For more information, see the [“spanning-tree mst root”](#) and the [“spanning-tree vlan”](#) sections.

If your network consists of switches that do not support the extended system ID and switches that do support it, it is unlikely that the switch with the extended system ID support will become the root switch. The extended system ID increases the switch priority value every time the VLAN number is greater than the priority of the connected switches.

Related Commands

Command	Description
show spanning-tree summary	Displays a summary of spanning-tree interface states.
spanning-tree mst root	Configures the MST root switch priority and timers based on the network diameter.
spanning-tree vlan priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree guard

Use the **spanning-tree guard** interface configuration command to enable root guard or loop guard on all the VLANs associated with the selected interface. Root guard restricts which interface is allowed to be the spanning-tree root port or the path-to-the root for the switch. Loop guard prevents alternate or root ports from becoming designated ports when a failure creates a unidirectional link. Use the **no** form of this command to return to the default setting.

spanning-tree guard {loop | none | root}

no spanning-tree guard

Syntax Description

loop	Enable loop guard.
none	Disable root guard or loop guard.
root	Enable root guard.

Defaults

Root guard is disabled.

Loop guard is configured according to the **spanning-tree loopguard default** global configuration command (globally disabled).

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

You can enable root guard or loop guard when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode.

When root guard is enabled, if spanning-tree calculations cause an interface to be selected as the root port, the interface transitions to the root-inconsistent (blocked) state to prevent the customer's switch from becoming the root switch or being in the path to the root. The root port provides the best path from the switch to the root switch.

When the **no spanning-tree guard** or the **no spanning-tree guard none** command is entered, root guard is disabled for all VLANs on the selected interface. If this interface is in the root-inconsistent (blocked) state, it automatically transitions to the listening state.

Do not enable root guard on interfaces that will be used by the UplinkFast feature. With UplinkFast, the backup ports (in the blocked state) replace the root port in the case of a failure. However, if root guard is also enabled, all the backup ports used by the UplinkFast feature are placed in the root-inconsistent state (blocked) and prevented from reaching the forwarding state. The UplinkFast feature is not available when the switch is operating in the rapid-PVST+ or MST mode.

Loop guard is most effective when it is configured on the entire switched network. When the switch is operating in PVST+ or rapid-PVST+ mode, loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send bridge protocol data units (BPDUs) on root or alternate

ports. When the switch is operating in MST mode, BPDUs are not sent on nonboundary interfaces if the interface is blocked by loop guard in all MST instances. On a boundary interface, loop guard blocks the interface in all MST instances.

To disable root guard or loop guard, use the **spanning-tree guard none** interface configuration command. You cannot enable both root guard and loop guard at the same time.

You can override the setting of the **spanning-tree loopguard default** global configuration command by using the **spanning-tree guard loop** interface configuration command.

Examples

This example shows how to enable root guard on all the VLANs associated with the specified port:

```
Switch(config)# interface fastethernet1/0/3
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 fastethernet1/0/3
Switch(config-if)# spanning-tree guard loop
```

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

Related Commands

Command	Description
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.
spanning-tree cost	Sets the path cost for spanning-tree calculations.
spanning-tree loopguard default	Prevents alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link.
spanning-tree mst cost	Configures the path cost for MST calculations.
spanning-tree mst port-priority	Configures an interface priority.
spanning-tree mst root	Configures the MST root switch priority and timers based on the network diameter.
spanning-tree port-priority	Configures an interface priority.
spanning-tree vlan priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree link-type

Use the **spanning-tree link-type** interface configuration command to override the default link-type setting, which is controlled by the duplex mode of the interface, and to enable rapid spanning-tree transitions to the forwarding state. Use the **no** form of this command to return to the default setting.

spanning-tree link-type { point-to-point | shared }

no spanning-tree link-type

Syntax Description	point-to-point	Specify that the link type of an interface is point-to-point.
	shared	Specify that the link type of an interface is shared.

Defaults	The switch derives the link type of an interface from the duplex mode. A full-duplex interface is considered a point-to-point link, and a half-duplex interface is considered a shared link.

Command Modes	Interface configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	You can override the default setting of the link type by using the spanning-tree link-type command; for example, a half-duplex link can be physically connected point-to-point to a single interface on a remote switch running the Multiple Spanning Tree Protocol (MSTP) or the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol and be enabled for rapid transitions.

Examples	This example shows how to specify the link type as shared (regardless of the duplex setting) and to prevent rapid transitions to the forwarding state:
	<pre>Switch(config-if)# spanning-tree link-type shared</pre>
	You can verify your setting by entering the show spanning-tree mst interface interface-id or the show spanning-tree interface interface-id privileged EXEC command.

Related Commands

Command	Description
clear spanning-tree detected-protocols	Restarts the protocol migration process (force the renegotiation with neighboring switches) on all interfaces or on the specified interface.
show spanning-tree interface <i>interface-id</i>	Displays spanning-tree state information for the specified interface.
show spanning-tree mst interface <i>interface-id</i>	Displays multiple spanning-tree (MST) information for the specified interface.

spanning-tree loopguard default

Use the **spanning-tree loopguard default** global configuration command to prevent alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link. Use the **no** form of this command to return to the default setting.

spanning-tree loopguard default

no spanning-tree loopguard default

Syntax Description This command has no arguments or keywords.

Defaults Loop guard is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines You can enable the loop guard feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode.

Loop guard is most effective when it is configured on the entire switched network. When the switch is operating in PVST+ or rapid-PVST+ mode, loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send bridge protocol data units (BPDUs) on root or alternate ports. When the switch is operating in MST mode, BPDUs are not sent on nonboundary interfaces if the interface is blocked by loop guard in all MST instances. On a boundary interface, loop guard blocks the interface in all MST instances.

Loop guard operates only on interfaces that are considered point-to-point by the spanning tree.

You can override the setting of the **spanning-tree loopguard default** global configuration command by using the **spanning-tree guard loop** interface configuration command.

Examples This example shows how to globally enable loop guard:

```
Switch(config)# spanning-tree loopguard default
```

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

Related Commands	Command	Description
	show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.
	spanning-tree guard loop	Enables the loop guard feature on all the VLANs associated with the specified interface.

spanning-tree mode

Use the **spanning-tree mode** global configuration command to enable per-VLAN spanning-tree plus (PVST+), rapid PVST+, or multiple spanning tree (MST) on your switch. Use the **no** form of this command to return to the default setting.

spanning-tree mode {mst | pvst | rapid-pvst}

no spanning-tree mode

Syntax Description	mst	Enable MST and Rapid Spanning Tree Protocol (RSTP) (based on IEEE 802.1s and IEEE 802.1w).
	pvst	Enable PVST+ (based on IEEE 802.1D).
	rapid-pvst	Enable rapid PVST+ (based on IEEE 802.1w).

Defaults The default mode is PVST+.

Command Modes Global configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines The switch supports PVST+, rapid PVST+, and MSTP, but only one version can be active at any time: All VLANs run PVST+, all VLANs run rapid PVST+, or all VLANs run MSTP.

When you enable the MST mode, RSTP is automatically enabled.



Caution

Changing spanning-tree modes can disrupt traffic because all spanning-tree instances are stopped for the previous mode and restarted in the new mode.

Examples This example shows to enable MST and RSTP on the switch:

```
Switch(config)# spanning-tree mode mst
```

This example shows to enable rapid PVST+ on the switch:

```
Switch(config)# spanning-tree mode rapid-pvst
```

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

Related Commands	Command	Description
	show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_comm_and_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.

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
12.1(14)AX	This command was introduced.
12.2(25)SEG	The <i>instance-id</i> range changed to 0 to 4094.

Usage Guidelines

The **spanning-tree mst configuration** command enables the MST configuration mode. These configuration commands are available:

- **abort**: exits the MST region configuration mode without applying configuration changes.
- **exit**: exits the MST region configuration mode and applies all configuration changes.
- **instance** *instance-id* **vlan** *vlan-range*: maps VLANs to an MST instance. The range for the *instance-id* is 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  Vlan Mapped
-----
0          1-9,21-4094
1          10-20
-----

Switch(config-mst)# exit
Switch(config)#
```

This example shows how to add VLANs 1 to 100 to the ones already mapped (if any) to instance 2, to move VLANs 40 to 60 that were previously mapped to instance 2 to the CIST instance, to add VLAN 10 to instance 10, and to remove all the VLANs mapped to instance 2 and map them to the CIST instance:

```
Switch(config-mst)# instance 2 vlan 1-100
Switch(config-mst)# no instance 2 vlan 40-60
Switch(config-mst)# instance 10 vlan 10
Switch(config-mst)# no instance 2
```

You can verify your settings by entering the **show pending** MST configuration command.

Related Commands

Command	Description
show spanning-tree mst configuration	Displays the MST region configuration.

spanning-tree mst cost

Use the **spanning-tree mst cost** interface configuration command to set the path cost for multiple spanning-tree (MST) calculations. If a loop occurs, spanning tree considers the path cost when selecting an interface to put in the forwarding state. Use the **no** form of this command to return to the default setting.

spanning-tree mst *instance-id* **cost** *cost*

no spanning-tree mst *instance-id* **cost**

Syntax Description	<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>cost</i>	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
	12.1(14)AX	This command was introduced.
	12.2(25)SEG	The <i>instance-id</i> range changed to 0 to 4094.

Usage Guidelines	When you configure the cost, higher values represent higher costs.

Examples	This example shows how to set a path cost of 250 on a port associated with instances 2 and 4: <pre>Switch(config)# interface fastethernet1/0/4 Switch(config-if)# spanning-tree mst 2,4 cost 250</pre> You can verify your settings by entering the show spanning-tree mst interface <i>interface-id</i> privileged EXEC command.

Related Commands	Command	Description
	show spanning-tree mst interface <i>interface-id</i>	Displays MST information for the specified interface.
	spanning-tree mst port-priority	Configures an interface priority.
	spanning-tree mst priority	Configures the switch priority for the specified spanning-tree instance.

spanning-tree mst forward-time

Use the **spanning-tree mst forward-time** global configuration command to set the forward-delay time for all multiple spanning-tree (MST) instances. The forwarding time controls how long each of the listening and learning states last before the interface begins forwarding. Use the **no** form of this command to return to the default setting.

spanning-tree mst forward-time *seconds*

no spanning-tree mst forward-time

Syntax Description	<i>seconds</i>	Length of the listening and learning states. The range is 4 to 30 seconds.

Defaults	The default is 15 seconds.

Command Modes	Global configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	Changing the spanning-tree mst forward-time command affects all spanning-tree instances.

Examples	This example shows how to set the spanning-tree forwarding time to 18 seconds for all MST instances:
	Switch(config)# spanning-tree mst forward-time 18
	You can verify your setting by entering the show spanning-tree mst privileged EXEC command.

Related Commands	Command	Description
	show spanning-tree mst	Displays MST information.
	spanning-tree mst hello-time	Sets the interval between hello bridge protocol data units (BPDUs) sent by root switch configuration messages.
	spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
	spanning-tree mst max-hops	Sets the number of hops in a region before the BPDU is discarded.

spanning-tree mst hello-time

Use the **spanning-tree mst hello-time** global configuration command to set the interval between hello bridge protocol data units (BPDUs) sent by root switch configuration messages. Use the **no** form of this command to return to the default setting.

spanning-tree mst hello-time *seconds*

no spanning-tree mst hello-time

Syntax Description	<i>seconds</i>	Interval between hello BPDUs sent by root switch configuration messages. The range is 1 to 10 seconds.

Defaults	The default is 2 seconds.

Command Modes	Global configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	After you set the spanning-tree mst max-age <i>seconds</i> global configuration command, if a switch does not receive BPDUs from the root switch within the specified interval, the switch recomputes the spanning-tree topology. The max-age setting must be greater than the hello-time setting. Changing the spanning-tree mst hello-time command affects all spanning-tree instances.

Examples	This example shows how to set the spanning-tree hello time to 3 seconds for all multiple spanning-tree (MST) instances:

```
Switch(config)# spanning-tree mst hello-time 3
```

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

Related Commands	Command	Description
	show spanning-tree mst	Displays MST information.
	spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
	spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
	spanning-tree mst max-hops	Sets the number of hops in a region before the BPDU is discarded.

spanning-tree mst max-age

Use the **spanning-tree mst max-age** global configuration command to set the interval between messages that the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputes the spanning-tree topology. Use the **no** form of this command to return to the default setting.

spanning-tree mst max-age *seconds*

no spanning-tree mst max-age

Syntax Description	<i>seconds</i> Interval between messages the spanning tree receives from the root switch. The range is 6 to 40 seconds.

Defaults	The default is 20 seconds.

Command Modes	Global configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	After you set the spanning-tree mst max-age <i>seconds</i> global configuration command, if a switch does not receive BPDUs from the root switch within the specified interval, the switch recomputes the spanning-tree topology. The max-age setting must be greater than the hello-time setting. Changing the spanning-tree mst max-age command affects all spanning-tree instances.

Examples	This example shows how to set the spanning-tree max-age to 30 seconds for all multiple spanning-tree (MST) instances:

```
Switch(config)# spanning-tree mst max-age 30
```

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

Related Commands	Command	Description
	show spanning-tree mst	Displays MST information.
	spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
	spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
	spanning-tree mst max-hops	Sets the number of hops in a region before the BPDU is discarded.

spanning-tree mst max-hops

Use the **spanning-tree mst max-hops** global configuration command to set the number of hops in a region before the bridge protocol data unit (BPDU) is discarded and the information held for an interface is aged. Use the **no** form of this command to return to the default setting.

spanning-tree mst max-hops *hop-count*

no spanning-tree mst max-hops

Syntax Description	<i>hop-count</i> Number of hops in a region before the BPDU is discarded. The range is 1 to 255 hops.

Defaults	The default is 20 hops.

Command Modes	Global configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.
	12.2(25)SEG	The <i>hop-count</i> range changed to 1 to 255.

Usage Guidelines	The root switch of the instance always sends a BPDU (or M-record) with a cost of 0 and the hop count set to the maximum value. When a switch receives this BPDU, it decrements the received remaining hop count by one and propagates the decremented count as the remaining hop count in the generated M-records. When the count reaches 0, a switch discards the BPDU and ages the information held for the interface.

Changing the **spanning-tree mst max-hops** command affects all spanning-tree instances.

Examples	This example shows how to set the spanning-tree max-hops to 10 for all multiple spanning-tree (MST) instances:

```
Switch(config)# spanning-tree mst max-hops 10
```

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

Related Commands	Command	Description
	show spanning-tree mst	Displays MST information.
	spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
	spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
	spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.

spanning-tree mst 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(25)SEG	This command was introduced.

Usage Guidelines

The port can accept both prestandard and standard BPDUs. If the neighbor types are mismatched, only the common and internal spanning tree (CIST) runs on this interface.



Note

If a switch port is connected to a switch running prestandard Cisco IOS software, you *must* use the **spanning-tree mst pre-standard** interface configuration command on the port. If you do not configure the port to send only prestandard BPDUs, the Multiple STP (MSTP) performance might diminish.

When the port is configured to automatically detect prestandard neighbors, the *prestandard* flag always appears in the **show spanning-tree mst** commands.

Examples

This example shows how to configure a port to send only prestandard BPDUs:

```
Switch(config-if)# spanning-tree mst pre-standard
```

You can verify your settings by entering the **show spanning-tree mst** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree mst <i>instance-id</i>	Displays multiple spanning-tree (MST) information, including the <i>prestandard</i> flag, for the specified interface.

spanning-tree mst port-priority

Use the **spanning-tree mst port-priority** interface configuration command to configure an interface priority. If a loop occurs, the Multiple Spanning Tree Protocol (MSTP) can select which 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
	12.1(14)AX	This command was introduced.
	12.2(25)SEG	The <i>instance-id</i> range changed to 0 to 4094.

Usage Guidelines You can assign higher priority values (lower numerical values) to interfaces that you want selected first and lower priority values (higher numerical values) that you want selected last. If all interfaces have the same priority value, the multiple spanning tree (MST) puts the interface with the lowest interface number in the forwarding state and blocks other interfaces.

Examples This example shows how to increase the likelihood that the port associated with spanning-tree instances 20 and 22 is placed into the forwarding state if a loop occurs:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# spanning-tree mst 20,22 port-priority 0
```

You can verify your settings by entering the **show spanning-tree mst interface** *interface-id* privileged EXEC command.

Related Commands	Command	Description
	show spanning-tree mst interface <i>interface-id</i>	Displays MST information for the specified interface.
	spanning-tree mst cost	Sets the path cost for MST calculations.
	spanning-tree mst priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree mst priority

Use the **spanning-tree mst priority** global configuration command to set the switch priority for the specified spanning-tree instance. Use the **no** form of this command to return to the default setting.

spanning-tree mst *instance-id* **priority** *priority*

no spanning-tree mst *instance-id* **priority**

Syntax Description	<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>	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
	12.1(14)AX	This command was introduced.
	12.2(25)SEG	The <i>instance-id</i> range changed to 0 to 4094.

Examples This example shows how to set the spanning-tree priority to 8192 for multiple spanning-tree instances (MST) 20 to 21:

```
Switch(config)# spanning-tree mst 20-21 priority 8192
```

You can verify your settings by entering the **show spanning-tree mst instance-id** privileged EXEC command.

Related Commands	Command	Description
	show spanning-tree mst instance-id	Displays MST information for the specified interface.
	spanning-tree mst cost	Sets the path cost for MST calculations.
	spanning-tree mst port-priority	Configures an interface priority.

spanning-tree mst root

Use the **spanning-tree mst root** global configuration command to configure the multiple spanning-tree (MST) root switch priority and timers based on the network diameter. Use the **no** form of this command to return to the default settings.

spanning-tree mst *instance-id* **root** { **primary** | **secondary** } [**diameter** *net-diameter* [**hello-time** *seconds*]]

no spanning-tree mst *instance-id* **root**

Syntax Description

<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.
root primary	Force this switch to be the root switch.
root secondary	Set this switch to be the root switch should the primary root switch fail.
diameter <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.
hello-time <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
12.1(14)AX	This command was introduced.
12.2(25)SEG	The <i>instance-id</i> range changed to 0 to 4094.

Usage Guidelines

Use the **spanning-tree mst** *instance-id* **root** command only on backbone switches.

When you enter the **spanning-tree mst** *instance-id* **root** command, the software tries to set a high enough priority to make this switch the root of the spanning-tree instance. Because of the extended system ID support, the switch sets the switch priority for the instance to 24576 if this value will cause this switch to become the root for the specified instance. If any root switch for the specified instance has a switch priority lower than 24576, the switch sets its own priority to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value.)

When you enter the **spanning-tree mst *instance-id* root secondary** command, because of support for the extended system ID, the software changes the switch priority from the default value (32768) to 28672. If the root switch fails, this switch becomes the next root switch (if the other switches in the network use the default switch priority of 32768 and are therefore unlikely to become the root switch).

Examples

This example shows how to configure the switch as the root switch for instance 10 with a network diameter of 4:

```
Switch(config)# spanning-tree mst 10 root primary diameter 4
```

This example shows how to configure the switch as the secondary root switch for instance 10 with a network diameter of 4:

```
Switch(config)# spanning-tree mst 10 root secondary diameter 4
```

You can verify your settings by entering the **show spanning-tree mst *instance-id*** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree mst <i>instance-id</i>	Displays MST information for the specified instance.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
spanning-tree mst max-hops	Sets the number of hops in a region before the BPDU is discarded.

spanning-tree port-priority

Use the **spanning-tree port-priority** interface configuration command to configure an interface priority. If a loop occurs, spanning tree can select which interface to put in the forwarding state. Use the **no** form of this command to return to the default setting.

spanning-tree [**vlan** *vlan-id*] **port-priority** *priority*

no spanning-tree [**vlan** *vlan-id*] **port-priority**

Syntax Description

vlan <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
12.1(14)AX	This command was introduced.

Usage Guidelines

If the variable *vlan-id* is omitted, the command applies to the spanning-tree instance associated with VLAN 1.

You can set the priority on a VLAN that has no ports assigned to it. The setting takes effect when you assign the port to the VLAN.

If you configure an interface with both the **spanning-tree vlan** *vlan-id* **port-priority** *priority* command and the **spanning-tree port-priority** *priority* command, the **spanning-tree vlan** *vlan-id* **port-priority** *priority* command takes effect.

Examples

This example shows how to increase the likelihood that the specified port will be put in the forwarding state if a loop occurs:

```
Switch(config)# interface fastethernet1/0/2
Switch(config-if)# spanning-tree vlan 20 port-priority 0
```

This example shows how to set the port-priority value on VLANs 20 to 25:

```
Switch(config-if)# spanning-tree vlan 20-25 port-priority 0
```

You can verify your settings by entering the **show spanning-tree interface** *interface-id* privileged EXEC command.

Related Commands	Command	Description
	show spanning-tree interface <i>interface-id</i>	Displays spanning-tree information for the specified interface.
	spanning-tree cost	Sets the path cost for spanning-tree calculations.
	spanning-tree vlan priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree portfast (global configuration)

Use the **spanning-tree portfast** global configuration command to globally enable bridge protocol data unit (BPDU) filtering on Port Fast-enabled interfaces, the BPDU guard feature on Port Fast-enabled interfaces, or the Port Fast feature on all nontrunking interfaces. The BPDU filtering feature prevents the switch interface from sending or receiving BPDUs. The BPDU guard feature puts Port Fast-enabled interfaces that receive BPDUs in an error-disabled state. Use the **no** form of this command to return to the default settings.

spanning-tree portfast { bpdupfilter default | bpduguard default | default }

no spanning-tree portfast { bpdupfilter default | bpduguard default | default }

Syntax Description	bpdupfilter default	Globally enable BPDU filtering on Port Fast-enabled interfaces, and prevent the switch interface connected to end stations from sending or receiving BPDUs.
	bpduguard default	Globally enable the BPDU guard feature on Port Fast-enabled interfaces, and place the interfaces that receive BPDUs in an error-disabled state.
	default	Globally enable the Port Fast feature on all nontrunking interfaces.

Defaults The BPDU filtering, the BPDU guard, and the Port Fast features are disabled on all interfaces unless they are individually configured.

Command Modes Global configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines 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 bpdupfilter default** global configuration command to globally enable BPDU filtering on interfaces that are Port Fast-enabled (the interfaces are in a Port Fast-operational state). The interfaces still send a few BPDUs at link-up before the switch begins to filter outbound BPDUs. You should globally enable BPDU filtering on a switch so that hosts connected to switch interfaces do not receive BPDUs. If a BPDU is received on a Port Fast-enabled interface, the interface loses its Port Fast-operational status, and BPDU filtering is disabled.

You can override the **spanning-tree portfast bpdupfilter default** global configuration command by using the **spanning-tree bdpupfilter** interface configuration command.



Caution

Enabling BPDU filtering on an interface is the same as disabling spanning tree on it and can result in spanning-tree loops.

Use the **spanning-tree portfast bpduguard default** global configuration command to globally enable BPDU guard on interfaces that are in a Port Fast-operational state. In a valid configuration, Port Fast-enabled interfaces do not receive BPDUs. Receiving a BPDU on a Port Fast-enabled interface signals an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the interface in the error-disabled state. The BPDU guard feature provides a secure response to invalid configurations because you must manually put the interface back in service. Use the BPDU guard feature in a service-provider network to prevent an access port from participating in the spanning tree.

You can override the **spanning-tree portfast bpduguard default** global configuration command by using the **spanning-tree bdpuguard** interface configuration command.

Configure Port Fast only on interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation. A Port Fast-enabled interface moves directly to the spanning-tree forwarding state when linkup occurs without waiting for the standard forward-delay time. When Port Fast is enabled, the interface changes directly from a blocking state to a forwarding state without making the intermediate spanning-tree state changes.

You can override the **spanning-tree portfast default** global configuration command by using the **spanning-tree portfast** interface configuration command. You can use the **no spanning-tree portfast default** global configuration command to disable Port Fast on all interfaces unless they are individually configured with the **spanning-tree portfast** interface configuration command.

Examples

This example shows how to globally enable BPDU filtering:

```
Switch(config)# spanning-tree portfast bpdufilter default
```

This example shows how to globally enable BPDU guard:

```
Switch(config)# spanning-tree portfast bpduguard default
```

This example shows how to globally enable Port Fast on all nontrunking interfaces:

```
Switch(config)# spanning-tree portfast default
```

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

Related Commands

Command	Description
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.
spanning-tree bpdufilter	Prevents an interface from sending or receiving BPDUs.
spanning-tree bdpuguard	Puts an interface in the error-disabled state when it receives a BPDU.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface in all its associated VLANs.

spanning-tree portfast (interface configuration)

Use the **spanning-tree portfast** interface configuration command to enable the Port Fast feature on an interface in all its associated VLANs. When the Port Fast feature is enabled, the interface changes directly from a blocking state to a forwarding state without making the intermediate spanning-tree state changes. Use the **no** form of this command to return to the default setting.

spanning-tree portfast [**disable** | **trunk**]

no spanning-tree portfast

Syntax Description	disable	(Optional) Disable the Port Fast feature on the specified interface.
	trunk	(Optional) Enable the Port Fast feature on a trunking interface.

Defaults	The Port Fast feature is disabled on all interfaces; however, it is automatically enabled on dynamic-access ports.

Command Modes	Interface configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	Use this feature only on interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation.
	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 port.
	An interface with the Port Fast feature enabled moves directly to the spanning-tree forwarding state without the standard forward-time delay.
	You can use the spanning-tree portfast default global configuration command to globally enable the Port Fast feature on all nontrunking interfaces. However, the spanning-tree portfast interface configuration command can override the global setting.
	If you configure the spanning-tree portfast default global configuration command, you can enable Port Fast on an interface that is not a trunk interface by using the no spanning-tree portfast interface configuration command.
	The no spanning-tree portfast interface configuration command is the same as the spanning-tree portfast disable interface configuration command.

Examples

This example shows how to enable Port Fast on a port:

```
Switch(config)# interface fastethernet1/0/2
Switch(config-if)# spanning-tree portfast
```

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

Related Commands

Command	Description
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.
spanning-tree bpdufilter	Prevents an interface from sending or receiving bridge protocol data units (BPDUs).
spanning-tree bpduguard	Puts an interface in the error-disabled state when it receives a BPDU.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled interfaces or enables the Port Fast feature on all nontrunking interfaces.

spanning-tree uplinkfast

Use the **spanning-tree uplinkfast** global configuration command to accelerate the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself. Use the **no** form of this command to return to the default setting.

spanning-tree uplinkfast [**max-update-rate** *pkts-per-second*]

no spanning-tree uplinkfast [**max-update-rate**]

Syntax Description

max-update-rate *pkts-per-second* (Optional) The number of packets per second at which update packets are sent. The range is 0 to 32000.

Defaults

UplinkFast is disabled.
The update rate is 150 packets per second.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

Use this command only on access switches.

You can configure the UplinkFast feature for rapid-PVST+ or for multiple spanning-tree (MST) mode, but the feature remains disabled (inactive) until you change the spanning-tree mode to PVST+.

When you enable UplinkFast, it is enabled for the entire switch and cannot be enabled for individual VLANs.

When UplinkFast is enabled, the switch priority of all VLANs is set to 49152. If you change the path cost to a value less than 3000 and you enable UplinkFast or UplinkFast is already enabled, the path cost of all interfaces and VLAN trunks is increased by 3000 (if you change the path cost to 3000 or above, the path cost is not altered). The changes to the switch priority and the path cost reduces the chance that a switch will become the root switch.

When UplinkFast is disabled, the switch priorities of all VLANs and path costs of all interfaces are set to default values if you did not modify them from their defaults.

When spanning tree detects that the root port has failed, UplinkFast immediately switches over to an alternate root port, changing the new root port directly to FORWARDING state. During this time, a topology change notification is sent.

Do not enable the root guard on interfaces that will be used by the UplinkFast feature. With UplinkFast, the backup ports (in the blocked state) replace the root port in the case of a failure. However, if root guard is also enabled, all the backup ports used by the UplinkFast feature are placed in the root-inconsistent state (blocked) and prevented from reaching the forwarding state.

If you set the max-update-rate to 0, station-learning frames are not generated, so the spanning-tree topology converges more slowly after a loss of connectivity.

Examples

This example shows how to enable UplinkFast:

```
Switch(config)# spanning-tree uplinkfast
```

You can verify your setting by entering the **show spanning-tree summary** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree summary	Displays a summary of the spanning-tree interface states.
spanning-tree vlan root primary	Forces this switch to be the root switch.

spanning-tree vlan

Use the **spanning-tree vlan** global configuration command to configure spanning tree on a per-VLAN basis. Use the **no** form of this command to return to the default setting.

```
spanning-tree vlan vlan-id [forward-time seconds | hello-time seconds | max-age seconds |
priority priority | root {primary | secondary} [diameter net-diameter
hello-time seconds]]]
```

```
no spanning-tree vlan vlan-id [forward-time | hello-time | max-age | priority | root]
```

Syntax Description		
<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.
forward-time <i>seconds</i>		(Optional) Set the forward-delay time for the specified spanning-tree instance. The forwarding time controls how long each of the listening and learning states last before the interface begins forwarding. The range is 4 to 30 seconds.
hello-time <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.
max-age <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.
priority <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.
root primary		(Optional) Force this switch to be the root switch.
root secondary		(Optional) Set this switch to be the root switch should the primary root switch fail.
diameter <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
	12.1(14)AX	This command was introduced.

Usage Guidelines Disabling the STP causes the VLAN to stop participating in the spanning-tree topology. Interfaces that are administratively down remain down. Received BPDUs are forwarded like other multicast frames. The VLAN does not detect and prevent loops when STP is disabled.

You can disable the STP on a VLAN that is not currently active and verify the change by using the **show running-config** or the **show spanning-tree vlan *vlan-id*** privileged EXEC command. The setting takes effect when the VLAN is activated.

When disabling or re-enabling the STP, you can specify a range of VLANs that you want to disable or enable.

When a VLAN is disabled and then enabled, all assigned VLANs continue to be its members. However, all spanning-tree bridge parameters are returned to their previous settings (the last setting before the VLAN was disabled).

You can enable spanning-tree options on a VLAN that has no ports assigned to it. The setting takes effect when you assign ports to it.

When setting the **max-age *seconds***, if a switch does not receive BPDUs from the root switch within the specified interval, it recomputes the spanning-tree topology. The **max-age** setting must be greater than the **hello-time** setting.

The **spanning-tree vlan *vlan-id* root** command should be used only on backbone switches.

When you enter the **spanning-tree vlan *vlan-id* root** command, the software checks the switch priority of the current root switch for each VLAN. Because of the extended system ID support, the switch sets the switch priority for the specified VLAN to 24576 if this value will cause this switch to become the root for the specified VLAN. If any root switch for the specified VLAN has a switch priority lower than 24576, the switch sets its own priority for the specified VLAN to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value.)

When you enter the **spanning-tree vlan *vlan-id* root secondary** command, because of support for the extended system ID, the software changes the switch priority from the default value (32768) to 28672. If the root switch should fail, this switch becomes the next root switch (if the other switches in the network use the default switch priority of 32768, and therefore, are unlikely to become the root switch).

Examples This example shows how to disable the STP on VLAN 5:

```
Switch(config)# no spanning-tree vlan 5
```

You can verify your setting by entering the **show spanning-tree** privileged EXEC command. In this instance, VLAN 5 does not appear in the list.

This example shows how to set the spanning-tree forwarding time to 18 seconds for VLANs 20 and 25:

```
Switch(config)# spanning-tree vlan 20,25 forward-time 18
```

This example shows how to set the spanning-tree hello-delay time to 3 seconds for VLANs 20 to 24:

```
Switch(config)# spanning-tree vlan 20-24 hello-time 3
```


This example shows how to set spanning-tree max-age to 30 seconds for VLAN 20:

```
Switch(config)# spanning-tree vlan 20 max-age 30
```

This example shows how to reset the **max-age** parameter to the default value for spanning-tree instance 100 and 105 to 108:

```
Switch(config)# no spanning-tree vlan 100, 105-108 max-age
```

This example shows how to set the spanning-tree priority to 8192 for VLAN 20:

```
Switch(config)# spanning-tree vlan 20 priority 8192
```

This example shows how to configure the switch as the root switch for VLAN 10 with a network diameter of 4:

```
Switch(config)# spanning-tree vlan 10 root primary diameter 4
```

This example shows how to configure the switch as the secondary root switch for VLAN 10 with a network diameter of 4:

```
Switch(config)# spanning-tree vlan 10 root secondary diameter 4
```

You can verify your settings by entering the **show spanning-tree vlan *vlan-id*** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree vlan	Displays spanning-tree information.
spanning-tree cost	Sets the path cost for spanning-tree calculations.
spanning-tree guard	Enables the root guard or the loop guard feature for all the VLANs associated with the selected interface.
spanning-tree port-priority	Sets an interface priority.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled interfaces or enables the Port Fast feature on all nontrunking interfaces.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface in all its associated VLANs.
spanning-tree uplinkfast	Enables the UplinkFast feature, which accelerates the choice of a new root port.

speed

Use the **speed** interface configuration command to specify the speed of a 10/100 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

Syntax Description		
	10	Port runs at 10 Mbps.
	100	Port runs at 100 Mbps.
	1000	Port runs at 1000 Mbps. This option is valid and visible only on SFP module ports when the 1000BASE-T SFP module is inserted.
	auto	Port automatically detects the speed it should run at based on the port at the other end of the link. If you use the 10 , 100 , or 1000 keywords with the auto keyword, the port only autonegotiates at the specified speeds.
	nonegotiate	Autonegotiation is disabled, and the port runs at 1000 Mbps. This option is valid and visible only on SFP ports. (The 1000BASE-T SFP does not support the nonegotiate keyword.)

Defaults The default is **auto**.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.
	12.2(25)EY	Support for the 10 , 100 , and 1000 keywords with the auto keyword was added.

Usage Guidelines

For 10/100 Mbps ports, if both speed and duplex are set to specific values, the link operates at the negotiated speed and duplex value.

For 10/100/1000 Mbps ports, if both the speed and duplex are set to specific values, autonegotiation is disabled.

You can configure the Fast Ethernet port speed as either 10 or 100 Mbps. You cannot configure speed on SFP module ports, but you can configure speed to not negotiate (**nonegotiate**) if connected to a device that does not support autonegotiation. However, when a 1000BASE-T SFP module is in the SFP module port, you can configure speed as 10, 100, or 1000 Mbps or **auto**.

When a 1000BASE-T SFP module is inserted in an ES module port, the speed defaults to 1000.

**Caution**

Enhanced services (ES) ports do not support 10 or 100 Mbps operation. Setting the speed on an ES port to **auto** can result in severe data loss if the interface is connected to a 10/100 interface on another switch.

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, manually configure duplex and speed on the other side; do use the **auto** setting on the supported side.

**Caution**

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

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

Examples

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

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

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

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

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

Related Commands

Command	Description
duplex	Specifies the duplex mode of operation for Fast Ethernet and Gigabit Ethernet ports.
show interfaces	Displays the statistical information specific to all interfaces or to a specific interface.

srr-queue bandwidth limit

Use the **srr-queue bandwidth limit** interface configuration command to limit the maximum output on a standard port. Use the **no** form of this command to return to the default setting.

srr-queue bandwidth limit *weight1*

no srr-queue bandwidth limit

Syntax Description	<i>weight1</i>	Percentage of the port speed to which the standard port should be limited. The range is 10 to 90.

Defaults	The port is not rate-limited and is set to 100 percent.

Command Modes	Interface configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	If you configure this command to 80 percent, the port is idle 20 percent of the time. The line rate drops to 80 percent of the connected speed. These values are not exact because the hardware adjusts the line rate in increments of six.

This command is not supported on an enhanced-services (ES) port.



Note

The egress queue-set default settings are suitable for most situations. You should change them only when you have a thorough understanding of the queues and if these settings do not meet your quality of service (QoS) solution.

Examples	This example shows how to limit a port to 800 Mbps:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# srr-queue bandwidth limit 80
```

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

Related Commands

Command	Description
mls qos queue-set output buffers	Allocates buffers to the queue-set.
mls qos srr-queue output cos-map	Maps class of service (CoS) values to egress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue output dscp-map	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
mls qos queue-set output threshold	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation for the queue-set.
queue-set	Maps a port to a queue-set.
show mls qos interface queueing	Displays queueing strategy information.
srr-queue bandwidth shape	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a standard port.
srr-queue bandwidth share	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

srr-queue bandwidth shape

Use the **srr-queue bandwidth shape** interface configuration command to assign the shaped weights and to enable bandwidth shaping on the four egress queues mapped to a standard port. Use the **no** form of this command to return to the default setting.

```
srr-queue bandwidth shape weight1 weight2 weight3 weight4
```

```
no srr-queue bandwidth shape
```

Syntax Description

<i>weight1 weight2 weight3 weight4</i>	Specify the weights to control the percentage of the standard port that is shaped. The inverse ratio (<i>1/weight</i>) controls the shaping bandwidth for this queue. Separate each value with a space. The range is 0 to 65535.

Defaults

Weight1 is set to 25. Weight2, weight3, and weight4 are set to 0, and these queues are in shared mode.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

In shaped mode, the queues are guaranteed a percentage of the bandwidth, and they are rate-limited to that amount. Shaped traffic does not use more than the allocated bandwidth even if the link is idle. Use shaping to smooth bursty traffic or to provide a smoother output over time.

The shaped mode overrides the shared mode.

If you configure a shaped queue weight to 0 by using the **srr-queue bandwidth shape** interface configuration command, this queue participates in shared mode. The weight specified with the **srr-queue bandwidth shape** command is ignored, and the weights specified with the **srr-queue bandwidth share** interface configuration command for a queue come into effect.

When configuring queues for the same port for both shaping and sharing, make sure that you configure the lowest numbered queue for shaping.

This command is not supported on an enhanced-services (ES) port.

For information about the interaction between the **priority-queue** interface configuration command and the **srr-queue bandwidth shape** interface configuration command, see the usage guidelines in the [“priority-queue” section on page 2-327](#).



Note

The egress queue-set default settings are suitable for most situations. You should change them only when you have a thorough understanding of the queues and if these settings do not meet your quality of service (QoS) solution.

Examples

This example shows how to configure the queues for the same port for both shaping and sharing. Because the weight ratios for queues 2, 3, and 4 are set to 0, these queues operate in shared mode. The bandwidth weight for queue 1 is 1/8, which is 12.5 percent. Queue 1 is guaranteed this bandwidth and limited to it. It does not extend its slot to the other queues even if the other queues have no traffic and are idle. Queues 2, 3, and 4 are in shared mode, and the setting for queue 1 is ignored. The bandwidth ratio allocated for the queues in shared mode is $4/(4+4+4)$, which is 33 percent.

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# srr-queue bandwidth shape 8 0 0 0
Switch(config-if)# srr-queue bandwidth share 4 4 4 4
```

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

Related Commands

Command	Description
mls qos queue-set output buffers	Allocates buffers to a queue-set.
mls qos srr-queue output cos-map	Maps class of service (CoS) values to an egress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue output dscp-map	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
mls qos queue-set output threshold	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
priority-queue	Enables the egress priority queue on a port.
queue-set	Maps a port to a queue-set.
show mls qos interface queueing	Displays queueing strategy information.
srr-queue bandwidth share	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

srr-queue bandwidth share

Use the **srr-queue bandwidth share** interface configuration command to assign the shared weights and to enable bandwidth sharing on the four egress queues mapped to a port. The ratio of the weights is the ratio of frequency in which the shaped round robin (SRR) scheduler sends packets from each queue. Use the **no** form of this command to return to the default setting.

srr-queue bandwidth share *weight1 weight2 weight3 weight4*

no srr-queue bandwidth share

Syntax Description	<i>weight1 weight2 weight3 weight4</i> The ratios of <i>weight1</i> , <i>weight2</i> , <i>weight3</i> , and <i>weight4</i> control the ratio of the frequency in which the SRR scheduler sends packets. Separate each value with a space. The range is 1 to 255.					
Defaults	Weight1, weight2, weight3, and weight4 are 25 (1/4 of the bandwidth is allocated to each queue).					
Command Modes	Interface configuration					
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.1(14)AX</td><td>This command was introduced.</td></tr></table>	Release	Modification	12.1(14)AX	This command was introduced.	
Release	Modification					
12.1(14)AX	This command was introduced.					
Usage Guidelines	The absolute value of each weight is meaningless, and only the ratio of parameters is used. In shared mode, the queues share the bandwidth among them according to the configured weights. The bandwidth is guaranteed at this level but not limited to it. For example, if a queue empties and does not require a share of the link, the remaining queues can expand into the unused bandwidth and share it among themselves. If you configure a shaped queue weight to 0 by using the srr-queue bandwidth shape interface configuration command, this queue participates in SRR shared mode. The weight specified with the srr-queue bandwidth shape command is ignored, and the weights specified with the srr-queue bandwidth share interface configuration command for a queue take effect. When configuring queues for the same port for both shaping and sharing, make sure that you configure the lowest numbered queue for shaping. This command is supported on an enhanced-services (ES) port. For information about the interaction between the priority-queue interface configuration command and the srr-queue bandwidth share interface configuration command, see the usage guidelines in the “priority-queue” section on page 2-327.					
 Note	The egress queue-set default settings are suitable for most situations. You should change them only when you have a thorough understanding of the queues and if these settings do not meet your quality of service (QoS) solution.					

This example shows how to configure the weight ratio of the SRR scheduler running on an egress port. Four queues are used. The bandwidth ratio allocated for each queue in shared mode is $1/(1+2+3+4)$, $2/(1+2+3+4)$, $3/(1+2+3+4)$, and $4/(1+2+3+4)$, which is 10 percent, 20 percent, 30 percent, and 40 percent for queues 1, 2, 3, and 4. This means that queue 4 has four times the bandwidth of queue 1, twice the bandwidth of queue 2, and one-and-a-third times the bandwidth of queue 3.

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# srr-queue bandwidth share 1 2 3 4
```

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

Related Commands

Command	Description
mls qos queue-set output buffers	Allocates buffers to a queue-set.
mls qos srr-queue output cos-map	Maps class of service (CoS) values to an egress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue output dscp-map	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
mls qos queue-set output threshold	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
priority-queue	Enables the egress priority queue on a port.
queue-set	Maps a port to a queue-set.
show mls qos interface queueing	Displays queueing strategy information.
srr-queue bandwidth shape	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a standard port.

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

broadcast	Enable broadcast storm control on the interface.
multicast	Enable multicast storm control on the interface.
unicast	Enable unicast storm control on the interface.
level <i>level</i> [<i>level-low</i>]	Specify the rising and falling suppression levels as a percentage of total bandwidth of the port. <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. <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.
level bps <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. <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. <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. You can use metric suffixes such as k, m, and g for large number thresholds.
level pps <i>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. <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. <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. You can use metric suffixes such as k, m, and g for large number thresholds.

action { shutdown trap }	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. The keywords have these meanings: • shutdown—Disables the port during a storm. • trap—Sends an SNMP trap when a storm occurs.

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
12.1(14)AX	This command was introduced.
12.2(25)EY	The level <i>level</i> [<i>level</i>] options were replaced with the level { <i>level</i> [<i>level-low</i>] pps <i>pps</i> [<i>pps-low</i>] bps <i>bps</i> [<i>bps-low</i>] } action { shutdown trap } options.

Usage Guidelines

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.

**Note**

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.

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
show storm-control	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 on the switch stack or on a standalone switch 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

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 use this command before assigning an IP address to a routed port.

**Note**

If an interface is configured as a Layer 3 interface, you must first enter this **switchport** command with no keywords to configure the interface as a Layer 2 port. Then you can enter additional switchport commands with keywords, as shown on the pages that follow.

Syntax Description

This command has no arguments or keywords.

Defaults

By default, all interfaces are in Layer 2 mode.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

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.

Examples

This example shows how to cause an interface to cease operating as a Layer 2 port and become a Cisco-routed port:

```
Switch(config-if)# no switchport
```

This example shows how to cause the port interface to cease operating as a Cisco-routed port and convert to a Layer 2-switched interface:

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

**Note**

The **switchport** command without keywords is not used on platforms that do not support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 2-switched interfaces.

You can verify the switchport status of an interface by entering the **show running-config** privileged EXEC command.

Related Commands	Command	Description
	show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
	show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.

switchport access

Use the **switchport access** interface configuration command to configure a port as a static-access or dynamic-access port. If the switchport mode is set to **access**, the port operates as a member of the specified VLAN. If set to **dynamic**, the port starts discovery of VLAN assignment based on the incoming packets it receives. Use the **no** form of this command to reset the access mode to the default VLAN for the switch.

switchport access vlan {*vlan-id* | **dynamic**}

no switchport access vlan

Syntax Description		
vlan <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.
vlan dynamic		Specify that the access mode VLAN is dependent on the VLAN Membership Policy Server (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.

Defaults	The default access VLAN and trunk interface native VLAN is a default VLAN corresponding to the platform or interface hardware. A dynamic-access port is initially a member of no VLAN and receives its assignment based on the packet it receives.

Command Modes	Interface configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	The no switchport access command resets the access mode VLAN to the appropriate default VLAN for the device. The port must be in access mode before the switchport access vlan command can take effect. An access port can be assigned to only one VLAN. The VMPS server (such as a Catalyst 6500 series switch) must be configured before a port is configured as dynamic. These restrictions apply to dynamic-access ports: The software implements the VLAN Query Protocol (VQP) client, which can query a VMPS such as a Catalyst 6000 series switch. This 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.
- Configure the network so that STP does not put the dynamic-access port into an STP blocking state. The Port Fast feature is automatically enabled on dynamic-access ports.
- 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.
 - Tunnel ports.

Examples

This example shows how to cause a port interface that has already been configured as a switched interface to operate in VLAN 2 instead of the platform's default VLAN when in access mode:

```
Switch(config-if)# switchport access vlan 2
```

You can verify your setting by entering the **show interfaces *interface-id* switchport** privileged EXEC command and examining information in the Administrative Mode and Operational Mode rows.

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
switchport mode	Configures the VLAN membership mode of a port.

switchport backup interface



Note

To use this command, the switch must be running the LAN Base image.

Use the **switchport backup interface** interface configuration command on a Layer 2 interface 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 | TenGigabitEthernet 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 | TenGigabitEthernet interface-id] {mmu primary vlan
interface-id | multicast fast-convergence | preemption {delay delay-time | mode} | prefer
vlan vlan-id}
```

Syntax Description

FastEthernet	FastEthernet IEEE 802.3 port name. Valid range is 0 to 9.
GigabitEthernet	GigabitEthernet IEEE 802.3z port name. Valid range is 0 to 9.
Port-channel	Ethernet Channel of interface. Valid range is 0 to 48.
TenGigabitEthernet	Ten Gigabit Ethernet port name. Valid range is 0 to 9.
<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.
mmu	MAC-address move update. Configure the MAC move update (MMU) for a backup interface pair.
primary vlan <i>vlan-id</i>	The VLAN ID of the private-VLAN primary VLAN; valid range is 1 to 4,094.
multicast fast-convergence	Multicast Fast-convergence parameter.
preemption	Configure a preemption scheme for a backup interface pair.
delay <i>delay-time</i>	(Optional) Specify a preemption delay; the valid values are 1 to 300 seconds.
mode	Specify a preemption mode as bandwidth, forced, or off.
prefer vlan <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.
off	(Optional) Specify that no preemption occurs from backup to active.
delay <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(20)SE	This command was introduced.
12.2(25)FX	This command was introduced.
12.2(25)SEE	Added preemption , mode , forced , bandwidth , off , and delay keywords.
12.2(37)SE	Added prefer vlan keyword.
12.2(44)SE	The multicast , fast-convergence , delay , mode , prefer , and vlan keywords were added.

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 fastethernet1/0/1
Switch(conf-if)# switchport backup interface fastethernet1/0/2
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 fastethernet1/0/1
Switch(conf-if)# switchport backup interface fastethernet1/0/2 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 fastethernet1/0/1
Switch(conf-if)# switchport backup interface fastethernet1/0/2 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 fastethernet1/0/1
Switch(conf-if)# switchport backup interface fastethernet1/0/2 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 1/0/6
Switch(config-if)# switchport backup interface gigabitethernet 1/0/8 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 1/0/6
Switch(config-if)# switchport backup interface gigabitEthernet 1/0/8 prefer vlan
60,100-120
```

When both interfaces are up, Gi1/0/6 forwards traffic for VLANs 1 to 50, and Gi1/0/8 forwards traffic for VLANs 60 and 100 to 120.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
GigabitEthernet1/0/6	GigabitEthernet1/0/8	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 Gi1/0/6 goes down, Gi1/0/8 carries all VLANs of the Flex Link pair.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
GigabitEthernet1/0/6	GigabitEthernet1/0/8	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 Gi1/0/6 comes up, VLANs preferred on this interface are blocked on the peer interface Gi1/0/8 and forwarded on Gi1/0/6.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
GigabitEthernet1/0/6	GigabitEthernet1/0/8	Active Up/Backup Up

switchport backup interface

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 Gi1/0/11:

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet 1/0/11
Switch(config-if)# switchport backup interface gigabitEthernet 1/0/12 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

GigabitEthernet1/0/11	GigabitEthernet1/0/12	Active Up/Backup Standby
Preemption Mode : off		
Multicast Fast Convergence : On		
Bandwidth : 1000000 Kbit (Gi1/0/11), 1000000 Kbit (Gi1/0/12)		
Mac Address Move Update Vlan : auto		

Related Commands

Command	Description
show interfaces <i>[interface-id]</i> switchport backup	Displays the configured Flex Links and their status on the switch or for the specified interface.

Use the **switchport backup interface** interface configuration command on a Layer 2 interface 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 *{interface-id}* [**mmu primary vlan** *vlan-id* | **preemption** {**delay** *delay-time* | **mode** {**bandwidth** | **forced** | **off**}}] [**prefer vlan** *vlan-id*]

no switchport backup interface *{interface-id}* [**mmu primary vlan** | **preemption** {**delay** | **mode**}] [**prefer vlan** *vlan-id*]

Syntax Description

<i>interface-id</i>	Specifies 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 48.
mmu	(Optional) Specifies configuring the mac move update (MMU) for a backup interface pair.
primary vlan <i>vlan-id</i>	The VLAN ID of the private-VLAN primary VLAN; valid range is 1 to 4094.
preemption	(Optional) Specifies configuring a preemption scheme for a backup interface pair.
mode	Specifies a preemption mode as bandwidth, forced, or off.

prefer <i>vlan vlan-id</i>	Specify that VLANs are carried on the backup interfaces of a flexlink pair. VLAN ID range is 1 to 4094.
bandwidth	Specifies the interface with the higher available bandwidth always preempts the backup.
forced	Specifies the interface always preempts the backup.
off	Specifies no preemption occurs from backup to active.
delay <i>delay-time</i>	Specifies a preemption delay; valid values are 1 to 300 seconds.

**Note**

Though visible in the command-line help, VLAN interfaces are not supported.

Defaults

The default is to have no Flex Links defined.

No preemption occurs.

Preemption delay is set to 35 seconds.

The MAC address-table move update feature is not configured on the switch.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(25)EY	This command was introduced.
12.25(SEE)	The mmu primary vlan , preemption mode (bandwidth, forced, and off) and delay keywords were added.
12.2(37)SE	Added prefer vlan keyword.

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 takes over traffic forwarding.

- 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 primary 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.
- For Flex Link VLAN load balancing, you must choose the preferred VLANs on the backup interface.
- You cannot configure a preemption mechanism and VLAN load balancing for the same Flex Links pair.

Examples

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

```
Switch# configure terminal
Switch(config)# interface fastethernet1/0/1
Switch(config-if)# switchport backup interface fastethernet1/0/2
Switch(config-if)# end
```

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

```
Switch# configure terminal
Switch(config)# interface fastethernet1/0/1
Switch(config-if)# switchport backup interface fastethernet1/0/2 preempt forced
Switch(config-if)# end
```

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

```
Switch# configure terminal
Switch(config)# interface fastethernet1/0/1
Switch(config-if)# switchport backup interface fastethernet1/0/2 preempt delay 150
Switch(config-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 1/0/6
Switch(config-if)# switchport backup interface gigabitethernet 1/0/8 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 1 to 50, 60, and 100 to 120 are configured on the switch:

```
Switch(config)# interface gigabitEthernet 1/0/6
Switch(config-if)# switchport backup interface gigabitEthernet 1/0/8 prefer vlan
60,100-120
```

When both interfaces are up, Gi1/0/8 forwards traffic for VLANs 60 and 100 to 120 and Gi1/0/6 forwards traffic for VLANs 1 to 50.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
GigabitEthernet1/0/6	GigabitEthernet1/0/8	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 Gi1/0/6 goes down, Gi1/0/8 carries all VLANs of the Flex Link pair.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
GigabitEthernet1/0/6	GigabitEthernet1/0/8	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 Gi1/0/6 comes up, VLANs preferred on this interface are blocked on the peer interface Gi1/0/8 and forwarded on Gi1/0/6.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
GigabitEthernet1/0/6	GigabitEthernet1/0/8	Active Up/Backup Up

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120

```
Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
FastEthernet1/0/3	FastEthernet1/0/4	Active Down/Backup Up

Vlans Preferred on Active Interface: 1-2,5-4094
Vlans Preferred on Backup Interface: 3-4
Preemption Mode : off
Bandwidth : 10000 Kbit (Fa1/0/3), 100000 Kbit (Fa1/0/4)
Mac Address Move Update Vlan : auto

Related Commands

Command	Description
show interfaces [<i>interface-id</i>] switchport backup	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	multicast	Specify that unknown multicast traffic should be blocked.
	unicast	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
	12.1(14)AX	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.

Blocking unknown multicast or unicast traffic is not automatically enabled on protected ports; you must explicitly configure it.

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.

Related Commands	Command	Description
	show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.

switchport host

Use the **switchport host** interface configuration command to optimize a Layer 2 port for a host connection. The **no** form of this command has no affect on the system.

switchport host

Syntax Description

This command has no arguments or keywords.

Defaults

The default is for the port to not be optimized for a host connection.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

To optimize the port for a host connection, the **switchport host** command sets switch port mode to access, enables spanning tree Port Fast, and disables channel grouping. Only an end station can accept this configuration.

Because spanning tree Port Fast is enabled, you should enter the **switchport host** command only on ports that are connected to a single host. Connecting other switches, hubs, concentrators, or bridges to a fast-start port can cause temporary spanning-tree loops.

Enable the **switchport host** command to decrease the time that it takes to start up packet forwarding.

Examples

This example shows how to optimize the port configuration for a host connection:

```
Switch(config-if)# switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
Switch(config-if)#
```

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

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including switchport mode.

switchport mode

Use the **switchport mode** interface configuration command to configure the VLAN membership mode of a port. Use the **no** form of this command to reset the mode to the appropriate default for the device.

switchport mode { **access** | **dot1q-tunnel** | **dynamic** { **auto** | **desirable** } | **trunk** }

no switchport mode { **access** | **dot1q-tunnel** | **dynamic** | **trunk** }

Syntax Description		
access		Set the port to access mode (either static-access or dynamic-access, depending on the setting of the switchport access vlan interface configuration command). The port is set to access unconditionally and operates as a nontrunking, single VLAN interface that sends and receives nonencapsulated (nontagged) frames. An access port can be assigned to only one VLAN.
dot1q-tunnel		Set the port as an 802.1Q tunnel port.
dynamic auto		Set the interface trunking mode dynamic parameter to auto to specify that the interface convert the link to a trunk link. This is the default switchport mode.
dynamic desirable		Set the interface trunking mode dynamic parameter to desirable to specify that the interface actively attempt to convert the link to a trunk link.
trunk		Set the port to trunk unconditionally. The port is a trunking VLAN Layer 2 interface. The port sends and receives encapsulated (tagged) frames that identify the VLAN of origination. A trunk is a point-to-point link between two switches or between a switch and a router.

Defaults The default mode is **dynamic auto**.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines A configuration that uses the **access** or **trunk**, or **dot1q-tunnel** keywords takes effect only when you configure the port in the appropriate mode by using the **switchport mode** command. The static-access and trunk configuration are saved, but only one configuration is active at a time.

When you enter **access** mode, the interface changes to permanent nontrunking mode and negotiates to convert the link into a nontrunk link even if the neighboring interface does not agree to the change.

When you enter **trunk** mode, the interface changes to permanent trunking mode and negotiates to convert the link into a trunk link even if the interface connecting to it does not agree to the change.

When you enter **dynamic auto** mode, the interface converts the link to a trunk link if the neighboring interface is set to **trunk** or **desirable** mode.

When you enter **dynamic desirable** mode, the interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode.

To autonegotiate trunking, the interfaces must be in the same VTP domain. Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which is a point-to-point protocol. However, some internetworking devices might forward DTP frames improperly, which could cause misconfigurations. To avoid this, you should configure interfaces connected to devices that do not support DTP to not forward DTP frames, which disables DTP.

- If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.
- To enable trunking to a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands to cause the interface to become a trunk but to not generate DTP frames.

When you enter **dot1q-tunnel**, the port is set unconditionally as an 802.1Q tunnel port.

Access and trunk ports are mutually exclusive with tunnel ports.

Any 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 802.1Q header. This restriction applies to router ACLs, port ACLs, and VLAN maps.

The 802.1x feature interacts with switchport modes in these ways:

- If you try to enable 802.1x on a trunk port, an error message appears, and 802.1x is not enabled. If you try to change the mode of an 802.1x-enabled port to trunk, the port mode is not changed.
- If you try to enable 802.1x on a port set to **dynamic auto** or **dynamic desirable**, an error message appears, and 802.1x is not enabled. If you try to change the mode of an 802.1x-enabled port to **dynamic auto** or **dynamic desirable**, the port mode is not changed.
- If you try to enable 802.1x on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and 802.1x is not enabled. If you try to change an 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.

Configuring a port as an 802.1Q tunnel port has these restrictions:

- IP routing and fallback bridging are 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 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 802.1Q tunnel ports, see the software configuration guide for this release.

Examples

This example shows how to configure a port for access mode:

```
Switch(config-if)# switchport mode access
```

This example shows how set the interface to dynamic desirable mode:

```
Switch(config-if)# switchport mode dynamic desirable
```

This example shows how to configure a port for trunk mode:

```
Switch(config-if)# switchport mode trunk
```

This example shows how to configure a port as an 802.1Q tunnel port:

```
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.

Related Commands	Command	Description
	show dot1q tunnel	Displays information about 802.1Q tunnel ports on the switch.
	show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
	switchport access	Configures a port as a static-access or dynamic-access port.
	switchport trunk	Configures the trunk characteristics when an interface is in trunking mode.

switchport 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** form of this command to reset the mode to the appropriate default for the device.

switchport mode private-vlan { host | promiscuous }

no switchport mode private-vlan

Syntax Description

host	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.
promiscuous	Configure the interface as a private-VLAN promiscuous port. Promiscuous ports are members of private-VLAN primary VLANs.

Defaults

The default private-VLAN mode is neither host nor promiscuous.
The default switchport mode is **dynamic auto**.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(25)EY	This command was introduced.

Usage Guidelines

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
- Dynamic Trunking Protocol (DTP)
- Port Aggregation Protocol (PAgP)
- Link Aggregation Control Protocol (LACP)
- Multicast VLAN Registration (MVR)
- voice VLAN

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.

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 a port 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 a port 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 1/0/1
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 interface 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 fastethernet 1/0/2
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
private-vlan	Configures a VLAN as a community, isolated, or primary VLAN or associates a primary VLAN with secondary VLANs.
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including private VLAN configuration.
switchport private-vlan	Configures private VLAN associations and mappings between primary and secondary VLANs on an interface.

switchport nonegotiate

Use the **switchport nonegotiate** interface configuration command to specify that Dynamic Trunking Protocol (DTP) negotiation packets are not sent on the Layer 2 interface. The switch does not engage in DTP negotiation on this interface. Use the **no** form of this command to return to the default setting.

switchport nonegotiate

no switchport nonegotiate

Syntax Description

This command has no arguments or keywords.

Defaults

The default is to use DTP negotiation to determine trunking status.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The **no** form of the **switchport nonegotiate** command removes **nonegotiate** status.

This command is valid only when the interface switchport mode is access or trunk (configured by using the **switchport mode access** or the **switchport mode trunk** interface configuration command). This command returns an error if you attempt to execute it in **dynamic** (**auto** or **desirable**) mode.

Internetworking devices that do not support DTP might forward DTP frames improperly and cause misconfigurations. To avoid this, you should turn off DTP by using the **switchport no negotiate** command to configure the interfaces connected to devices that do not support DTP to not forward DTP frames.

When you enter the **switchport nonegotiate** command, DTP negotiation packets are not sent on the interface. The device does or does not trunk according to the **mode** parameter: **access** or **trunk**.

- If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.
- To enable trunking on a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands to cause the interface to become a trunk but to not generate DTP frames.

Examples

This example shows how to cause a port to refrain from negotiating trunking mode and to act as a trunk or access port (depending on the mode set):

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

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

switchport nonegotiate

Related Commands	Command	Description
	show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
	switchport mode	Configures the VLAN membership mode of a port.

switchport 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 [**aging**] [**mac-address** *mac-address* [**vlan** *vlan-id*] | **mac-address sticky** [*mac-address*]] [**maximum** *value* [**vlan** *vlan-list*]] [**violation** {**protect** | **restrict** | **shutdown**}]

no switchport port-security [**aging**] [**mac-address** *mac-address* [**vlan** *vlan-id*] | **mac-address sticky** [*mac-address*]] [**maximum** [**vlan** *vlan-list*]] [**violation** {**protect** | **restrict** | **shutdown**}]

Syntax Description	
aging	(Optional) See the switchport port-security aging command.
mac-address <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.
vlan <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.
mac-address sticky [<i>mac-address</i>]	(Optional) Enable the interface for <i>sticky learning</i> by entering only the mac-address sticky 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.
maximum <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 determined by the maximum number of available MAC addresses allowed in the system. This number is determined by the active Switch Database Management (SDM) template. See the sdm prefer command. This number represents the total of available MAC addresses, including those used for other Layer 2 functions and any other secure MAC addresses configured on interfaces. The default setting is 1.
vlan [<i>vlan-list</i>]	(Optional) For trunk ports, you can set the maximum number of secure MAC addresses on a VLAN. If the vlan keyword is not entered, the default value is used. vlan—set a per-VLAN maximum value. vlan <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.
violation	(Optional) Set the security violation mode or the action to be taken if port security is violated. The default is shutdown .

protect	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. Note We do not recommend configuring the protect mode on a trunk port. The protect mode disables learning when any VLAN reaches its maximum limit, even if the port has not reached its maximum limit.
restrict	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.
shutdown	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 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.

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
12.1(14)AX	This command was introduced.

Usage Guidelines

A secure port has the following limitations:

- A secure port can be an access port or a trunk port; it cannot be a dynamic access port.
- A secure port cannot be a routed port.
- A secure port cannot be a protected port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- A secure port cannot belong to a Fast EtherChannel or a Gigabit EtherChannel port group.

- You cannot configure static secure or sticky secure MAC addresses in the voice VLAN.
- When you enable port security on an interface that is also configured with a voice VLAN, set the maximum allowed secure addresses on the port to two. When the port is connected to a Cisco IP phone, the IP phone requires one MAC address. The Cisco IP phone address is learned on the voice VLAN, but is not learned on the access VLAN. If you connect a single PC to the Cisco IP phone, no additional MAC addresses are required. If you connect more than one PC to the Cisco IP phone, you must configure enough secure addresses to allow one for each PC and one for the Cisco IP phone.
- If any type of port security is enabled on the access VLAN, dynamic port security is automatically enabled on the voice VLAN. You cannot configure port security on a per-VLAN basis.



Note Voice VLAN is supported only on access ports and not on trunk ports.

- When a voice VLAN is configured on a secure port that is also configured as a sticky secure port, all addresses on the voice VLAN are learned as dynamic secure addresses, and all addresses seen on the access VLAN to which the port belongs are learned as sticky secure addresses.
- You cannot configure static secure MAC addresses in the voice VLAN.
- 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 fastethernet1/0/12
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 gigabitethernet1/0/12
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:

```
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
show port-security address	Displays all the secure addresses configured on the switch.
show port-security interface interface-id	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

static	Enable aging for statically configured secure addresses on this port.
time <i>time</i>	Specify the aging time for this port. The range is 1 to 1440 minutes.
type	Set the aging type.
absolute	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.
inactivity	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
12.1(14)AX	This command was introduced.

Usage Guidelines

To enable secure address aging for a particular port, set the aging time to a value other than 0 for that port.

To allow limited time access to particular secure addresses, set the aging type as **absolute**. When the aging time lapses, the secure addresses are deleted.

To allow continuous access to a limited number of secure addresses, set the aging type as **inactivity**. This removes the secure address when it become inactive, and other addresses can become secure.

To allow unlimited access to a secure address, configure it as a secure address, and disable aging for the statically configured secure address by using the **no switchport port-security aging static** interface configuration command.

Examples

This example sets the aging time as 2 hours for absolute aging for all the secure addresses on a port:

```
Switch(config)# interface gigabitethernet1/0/1
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 a port:

```
Switch(config)# interface gigabitethernet1/0/2
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-if)# no switchport port-security aging static
```

Related Commands

Command	Description
show port-security	Displays the port security settings defined for the port.
switchport port-security	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 priority extend

Use the **switchport priority extend** interface configuration command to set a port priority for the incoming untagged frames or the priority of frames received by the IP phone connected to the specified port. Use the **no** form of this command to return to the default setting.

switchport priority extend {cos value | trust}

no switchport priority extend

Syntax Description

cos value	Set the IP phone port to override the 802.1p priority received from the PC or the attached device with the specified class of service (CoS) value. The range is 0 to 7. Seven is the highest priority. The default is 0.
trust	Set the IP phone port to trust the 802.1p priority received from the PC or the attached device.

Defaults

The default port priority is set to a CoS value of 0 for untagged frames received on the port.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

When voice VLAN is enabled, you can configure the switch to send the Cisco Discovery Protocol (CDP) packets to instruct the IP phone how to send data packets from the device attached to the access port on the Cisco IP Phone. You must enable CDP on the switch port connected to the Cisco IP Phone to send the configuration to the Cisco IP Phone. (CDP is enabled by default globally and on all switch interfaces.)

You should configure voice VLAN on switch access ports. You can only configure a voice VLAN on Layer 2 ports.

Before you enable voice VLAN, we recommend that you enable quality of service (QoS) on the switch by entering the **mls qos** global configuration command and configure the port trust state to trust by entering the **mls qos trust cos** interface configuration command.

Examples

This example shows how to configure the IP phone connected to the specified port to trust the received 802.1p priority:

```
Switch(config-if)# switchport priority extend trust
```

You can verify your settings by entering the **show interfaces interface-id switchport** privileged EXEC command.

 `switchport priority extend`

Related Commands	Command	Description
	show interfaces	Displays the administrative and operational status of a switching (nonrouting) port.
	switchport voice vlan	Configures the voice VLAN on the port.

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}
```

Syntax	Description
association	Define a private-VLAN association for a port.
host	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.
mapping	Define private-VLAN mapping for a promiscuous port.
add	Associate secondary VLANs to the primary VLAN.
remove	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.
host-association	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(25)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.

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 1/0/1
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 interface as a private-VLAN promiscuous port and map it to a primary VLAN and secondary VLANs:

```
Switch# configure terminal
Switch(config)# interface fastethernet 1/0/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 501-502
Switch(config-if)# end
```

You can verify private-VLAN mapping by using the **show interfaces private-vlan mapping** privileged EXEC command. You can verify private VLANs and interfaces configured on the switch stack by using the **show vlan private-vlan** privileged EXEC command.

Related Commands

Command	Description
show interfaces private-vlan mapping	Displays private VLAN mapping information for VLAN SVIs.
show vlan private-vlan	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

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
12.1(14)AX	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 unicast, multicast, or broadcast traffic to any other protected port. A protected port continues to forward unicast, multicast, and broadcast traffic to unprotected ports and vice versa.

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 a port:

```
Switch(config)# interface gigabitethernet1/0/2
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
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
switchport block	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* | **dot1q ethertype** *value* | **encapsulation** {**dot1q** | **isl** | **negotiate**} | **native vlan** *vlan-id* | **pruning vlan** *vlan-list*}

no switchport trunk {**allowed vlan** | **dot1q ethertype** *value* | **encapsulation** | **native vlan** | {**pruning vlan**}

Syntax Description

allowed vlan <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 none keyword is not valid. The default is all .
dot1q ethertype <i>value</i>	Sets the ethertype value on an enhanced-services (ES) port for 802.1Q encapsulation. Used to select a nonstandard (nondefault) 2-byte ethertype to identify 802.1Q tagged frames. The default ethertype value is 0x8100. Note This keyword is supported only on ES ports.
encapsulation	Set the encapsulation format on the trunk port. The default is to negotiate. Note Starting with release 12.2(25)EY, this keyword is not supported on ES ports. ES ports support only 802.1Q encapsulation.
dot1q	Set the encapsulation format on the trunk port to 802.1Q. With this format, the switch supports simultaneous tagged and untagged traffic on a port.
isl	Set the encapsulation format on the trunk port to Inter-Switch Link (ISL). The switch encapsulates all received and sent packets with an ISL header and filters native frames received from an ISL trunk port.
negotiate	Specify that the interface negotiate encapsulation with the neighboring interface. This is the default. If Dynamic Inter-Switch Link (DISL) and Dynamic Trunking Protocol (DTP) negotiation do not resolve the encapsulation format, ISL is the selected format.
native vlan <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.
pruning vlan <i>vlan-list</i>	Set the list of VLANs that are eligible for VTP pruning when in trunking mode. The all keyword is not valid.

The *vlan-list* format is **all** | **none** | [**add** | **remove** | **except**] *vlan-atom* [, *vlan-atom*...] where:

- **all** specifies all VLANs from 1 to 4094. This keyword is not allowed on commands that do not permit all VLANs in the list to be set at the same time.
- **none** means an empty list. This keyword is not allowed on commands that require certain VLANs to be set or at least one VLAN to be set.
- **add** adds the defined list of VLANs to those currently set instead of replacing the list. Valid IDs are from 1 to 1005; extended-range VLANs (VLAN IDs greater than 1005) are valid in some cases.



Note You can add extended-range VLANs to the allowed VLAN list, but not to the pruning-eligible VLAN list.

Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.

- **remove** removes the defined list of VLANs from those currently set instead of replacing the list. Valid IDs are from 1 to 1005; extended-range VLAN IDs are valid in some cases.



Note You can remove extended-range VLANs from the allowed VLAN list, but you cannot remove them from the pruning-eligible list.

Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.

- **except** lists the VLANs that should be calculated by inverting the defined list of VLANs. (VLANs are added except the ones specified.) Valid IDs are from 1 to 1005. Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.
- *vlan-atom* is either a single VLAN number from 1 to 4094 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen.

Defaults

The default encapsulation is negotiate.

VLAN 1 is the default native VLAN ID on the port.

The default for all VLAN lists is to include all VLANs.

The default ethertype value for 802.1Q encapsulation is 0x8100.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

Encapsulation:

- The **switchport trunk encapsulation** command is supported only on platforms and interface hardware that can support both ISL and 802.1Q formats.
- In Cisco IOS Release 12.2(25)EY and later, ISL encapsulation is supported only on standard ports and not on ES ports. ES ports support only 802.1Q encapsulation. When you upgrade a switch from Cisco IOS Release 12.2(14)AX to Cisco IOS Release 12.2(25)EY or later, during the initial configuration process the switchport trunk encapsulation option is rejected on ES ports and an error message is issued. You can ignore this error message. If you save the new configuration and later re-install the 12.1(14)AX image, the trunk encapsulation method originally configured on the ES ports is lost and the ES ports use the default encapsulation method, which is to negotiate.
- You cannot configure one end of the trunk as an 802.1Q trunk and the other end as an ISL or nontrunk port. However, you can configure one port as an ISL trunk and a different port on the same switch as an 802.1Q trunk.

- If you enter the **negotiate** keywords and DTP negotiation does not resolve the encapsulation format, ISL is the selected format. The **no** form of the command resets the trunk encapsulation format to the default.
- The **no** form of the **encapsulation** command resets the encapsulation format to the default.
- On an ES port, you can use the **switchport trunk dot1q ethertype value** interface configuration command to program a custom 802.1Q ethertype value on the interface. This feature allows the switch to interoperate with third-party vendor switches that do not use the standard 0x8100 ethertype to identify 802.1Q-tagged frames. For example, if you set 0x1234 as the custom 802.1Q ethertype on a trunk port, incoming frames containing that ethertype are assigned to the VLAN contained in the tag following the ethertype, as they would be with a standard 802.1Q trunk. Frames arriving on the trunk port containing any other ethertype are assigned to the native VLAN of that trunk.
- The **no switchport trunk dot1q ethertype** command resets the ethertype value to the default.

Native VLANs:

- All untagged traffic received on an 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 switch sends the packet without a tag; otherwise, the switch sends the packet with a tag.
- The **no** form of the **native vlan** command resets the native mode VLAN to the appropriate default VLAN for the device.

Allowed VLAN:

- To reduce the risk of spanning-tree loops or storms, you can disable VLAN 1 on any individual VLAN trunk port by removing VLAN 1 from the allowed list. When you remove VLAN 1 from a trunk port, the interface continues to send and receive management traffic, for example, Cisco Discovery Protocol (CDP), Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), Dynamic Trunking Protocol (DTP), and VLAN Trunking Protocol (VTP) in VLAN 1.
- The **no** form of the **allowed vlan** command resets the list to the default list, which allows all VLANs.

Trunk pruning:

- The pruning-eligible list applies only to trunk ports.
- Each trunk port has its own eligibility list.
- If you do not want a VLAN to be pruned, remove it from the pruning-eligible list. VLANs that are pruning-ineligible receive flooded traffic.
- VLAN 1, VLANs 1002 to 1005, and extended-range VLANs (VLANs 1006 to 4094) cannot be pruned.

Examples

This example shows how to cause a standard port configured as a switched interface to encapsulate in 802.1Q trunking format regardless of its default trunking format in trunking mode:

```
Switch(config-if)# switchport trunk encapsulation dot1q
```

This example shows how to configure VLAN 3 as the default port to send all untagged traffic:

```
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-if)# switchport trunk allowed vlan add 1,2,5,6
```

This example shows how to remove VLANs 3 and 10 to 15 from the pruning-eligible list:

```
Switch(config-if)# switchport trunk pruning vlan remove 3,10-15
```

You can verify your settings by entering the **show interfaces *interface-id* switchport** privileged EXEC command.

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
switchport mode	Configures the VLAN membership mode of a port.

switchport vlan mapping

Use the **switchport vlan mapping** interface configuration command on an enhanced-services (ES) port to map (or translate) customer VLANs to service-provider VLANs. Use the **no** form of this command to remove the VLAN mapping information.

switchport vlan mapping { *vlan-id translated-vlan-id* | **dot1q-tunnel** *outer-vlan-id* { *inner-vlan-id translated-vlan-id* | **drop** } | **internal dot1q-tunnel** *internal-outer-vlan-id internal-inner-vlan-id* **external dot1q-tunnel** *external-outer-vlan-id external-inner-vlan-id* }

no switchport vlan mapping { *vlan-id translated-vlan-id* | **dot1q-tunnel** *outer-vlan-id* { *inner-vlan-id translated-vlan-id* | **drop** } | **internal dot1q-tunnel** *internal-outer-vlan-id internal-inner-vlan-id* **external dot1q-tunnel** *external-outer-vlan-id external-inner-vlan-id* }

Syntax Description	
<i>vlan-id</i> <i>translated-vlan-id</i>	Configure the VLAN mapping on the interface as a one-to-one mapping. This maps the customer-side VLAN ID (<i>vlan-id</i>) to the service-provider side VLAN ID (<i>translated-vlan-id</i>). The customer-side VLAN ID is used to switch the packet inside the switch. The service-provider VLAN ID is sent or received on the ES ports. The VLAN ID range is from 1 to 4094.
dot1q-tunnel <i>outer-vlan-id</i> { <i>inner-vlan-id</i> <i>translated-vlan-id</i> drop }	Configure the 802.1Q tunnel VLAN mapping on the interface as a two-to-one mapping. The internal 802.1Q tunneling traffic with the outer VLAN ID (<i>outer-vlan-id</i>) and the inner VLAN ID (<i>inner-vlan-id</i>) is mapped to the service-provider VLAN ID (<i>translated-vlan-id</i>). The range is from 1 to 4094. Use the drop keyword to set the port to drop all VLAN traffic except for those VLANs that are explicitly mapped. Traffic with the specified outer VLAN ID is dropped unless the inner VLAN ID is matched in the existing VLAN mappings.
internal dot1q-tunnel <i>internal-outer-vlan-id</i> <i>internal-inner-vlan-id</i> external dot1q-tunnel <i>external-outer-vlan-id</i> <i>external-inner-vlan-id</i>	Configure the 802.1Q tunnel VLAN mapping as a two-to-two mapping. This maps 802.1Q tunneling traffic with the outer VLAN ID (<i>internal-outer-vlan-id</i>) and the inner VLAN ID (<i>internal-inner-vlan-id</i>) to the service-provider side VLAN outer ID (<i>external-outer-vlan-id</i>) and the VLAN inner ID (<i>external-inner-vlan-id</i>). The 802.1Q VLAN ID is used to switch the packet inside the switch. The service-provider VLAN ID is sent or received on the ES ports. The range is from 1 to 4094. Note The <i>external-inner-vlan-id</i> VLAN ID must be the same as the <i>internal-inner-vlan-id</i> VLAN ID.

Defaults No VLAN maps are configured.

Command Modes Interface configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.
12.2(25)EY	The internal dot1q-tunnel <i>internal-outer-vlan-id internal-inner-vlan-id</i> external dot1q-tunnel <i>external-outer-vlan-id external-inner-vlan-id</i> keywords were added.

Usage Guidelines

Use the **switchport vlan mapping** command only on ES ports that are attached to the service-provider network.

VLAN mapping acts as a filter on the ES ports and does not affect the internal operation of the switch. The VLAN ID in the 802.1Q tag is mapped just before a packet is sent or just after a packet is received on the ES port.

The service-provider VLANs are not visible to the switch, so all configuration and statistics relate to the customer-side VLANs. For example, an input access control list (ACL) on the ES port would be applied to the customer-side VLAN after it is mapped from the service-provider-side VLAN.

To configure a one-to-one VLAN mapping, use the *vlan-id translated-vlan-id* keywords. To configure a two-to-one VLAN mapping, use the **dot1q-tunnel** *outer-vlan-id inner-vlan-id translated-vlan-id* keywords. To configure two-to-two VLAN mapping, use the **internal dot1q-tunnel** *internal-outer-vlan-id internal-inner-vlan-id* **external dot1q-tunnel** *external-outer-vlan-id external-inner-vlan-id* keywords.

You can use the **switchport vlan mapping dot1q-tunnel** command to translate the outer VLAN and the inner VLAN in an 802.1Q tunnel to the service-provider VLAN. The switch can then translate overlapping customer VLANs by encapsulating the customer traffic in 802.1Q tunnels. Use the **drop** keyword to drop all VLAN traffic except traffic that is explicitly mapped.

When using the use the **switchport vlan mapping internal dot1q-tunnel** *internal-outer-vlan-id internal-inner-vlan-id* **external dot1q-tunnel** *external-outer-vlan-id external-inner-vlan-id* command, make sure that the inner VLAN ID of the original 802.1Q packet (*internal-inner-vlan-id*) and the inner VLAN ID in the service-provide network (*external-inner-vlan-id*) match. All switch configurations and actions, including QoS actions, apply to the 802.1Q inner and outer VLANs.

Examples

This example shows how to configure an interface so that 802.1Q traffic with the outer VLAN ID 5 and the inner VLAN ID 6 would leave the switch with the single VLAN ID 10 (a two-to-one mapping). The 802.1Q traffic with the outer VLAN 5 and any inner VLAN ID other than 6 would be dropped. Other traffic on VLAN 5 would also be dropped.

```
Switch(config)# interface gigabitethernet1/1/2
Switch(config-if)# switchport vlan mapping dot1q-tunnel 5 6 10
Switch(config-if)# switchport vlan mapping dot1q-tunnel 5 drop
```

This example shows how to map the outer and inner VLAN IDs of the original 802.1Q packet to the outer and inner VLAN IDs in the service-provider network (a two-to-two mapping).

```
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# switchport vlan mapping internal dot1q-tunnel 5 6 external dot1q tunnel
15 6
```

Related Commands	Command	Description
	show interfaces <i>interface-id</i> vlan mapping	Displays the VLAN mapping table for the identified interface.
	show vlan mapping	Displays the VLAN mapping table for the ES ports.
	switchport mode dot1q-tunnel	Configures an interface as an 802.1Q tunnel port.

switchport voice vlan

Use the **switchport voice vlan** interface configuration command to configure voice VLAN on the port. Use the **no** form of this command to return to the default setting.

switchport voice vlan {*vlan-id* | **dot1p** | **none** | **untagged**}

no switchport voice vlan

Syntax Description	
<i>vlan-id</i>	Specify the VLAN to be used for voice traffic. The range is 1 to 4094. By default, the IP phone forwards the voice traffic with an 802.1Q priority of 5.
dot1p	Configure the telephone to use 802.1p priority tagging and uses VLAN 0 (the native VLAN). By default, the Cisco IP phone forwards the voice traffic with an 802.1p priority of 5.
none	Do not instruct the IP telephone about the voice VLAN. The telephone uses the configuration from the telephone key pad.
untagged	Configure the telephone to send untagged voice traffic. This is the default for the telephone.

Defaults	The switch default is not to automatically configure the telephone (none). The telephone default is not to tag frames.

Command Modes	Interface configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	You should configure voice VLAN on Layer 2 access ports. You must enable Cisco Discovery Protocol (CDP) on the switchport connected to the Cisco IP phone for the switch to send configuration information to the phone. CDP is enabled by default globally and on the interface. Before you enable voice VLAN, we recommend you enable quality of service (QoS) on the switch by entering the mls qos global configuration command and configure the port trust state to trust by entering the mls qos trust cos interface configuration command. When you enter a VLAN ID, the IP phone forwards voice traffic in 802.1Q frames, tagged with the specified VLAN ID. The switch puts 802.1Q voice traffic in the voice VLAN. When you select dot1p, none, or untagged, the switch puts the indicated voice traffic in the access VLAN. In all configurations, the voice traffic carries a Layer 2 IP precedence value. The default is 5 for voice traffic.

When you enable port security on an interface that is also configured with a voice VLAN, set the maximum allowed secure addresses on the port to two. When the port is connected to a Cisco IP phone, the IP phone requires up to two MAC addresses. The IP phone address is learned on the voice VLAN, but is not learned on the access VLAN. If you connect a single PC to the Cisco IP phone, no additional MAC addresses are required. If you connect more than one PC to the Cisco IP phone, you must configure enough secure addresses to allow one for each PC and one for the Cisco IP phone.

If any type of port security is enabled on the access VALN, dynamic port security is automatically enabled on the voice VLAN.

You cannot configure static secure MAC addresses in the voice VLAN.

The Port Fast feature is automatically enabled when voice VLAN is configured. When you disable voice VLAN, the Port Fast feature is not automatically disabled.

Examples

This example shows how to configure VLAN 2 as the voice VLAN on a port:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport voice vlan 2
```

You can verify your settings by entering the **show interfaces interface-id switchport** privileged EXEC command.

Related Commands

Command	Description
show interfaces interface-id switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport priority extend	Determines how the device connected to the specified port handles priority traffic received on its incoming port.

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, for Fast Ethernet (10/100) ports, or for routed ports. Use the **no** form of this command to restore the global MTU value to its default value.

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

no system mtu

Syntax Description

<i>bytes</i>	Set the system MTU for Fast Ethernet (10/100) ports. The range is 1500 to 1998 bytes.
jumbo bytes	Set the system jumbo frame size (MTU) for Gigabit Ethernet ports. The range is 1500 to 9000 bytes.
routing bytes	Set the system MTU for routed ports. The range is 1500 to the system MTU value. This is the maximum MTU that can be routed for all ports. Although larger packets can be accepted, they cannot be routed.

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
12.1(14)AX	This command was introduced.
12.2(25)SED	The <i>bytes</i> range is now 1500 to 1998. The routing bytes keywords were added.

Usage Guidelines

When you use this command to change the 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. Unlike the system MTU routing configuration, the MTU settings you enter with the **system mtu** and **system mtu jumbo** commands are not saved in the switch IOS configuration file, even if you enter the **copy running-config startup-config** privileged EXEC command. Therefore, if you use TFTP to configure a new switch by using a backup configuration file and want the system MTU to be other than the default, you must explicitly configure the **system mtu** and **system mtu jumbo** settings on the new switch and then reload the switch.

Gigabit Ethernet ports are not affected by the **system mtu** command; Fast Ethernet 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 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.

**Note**

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

The size of frames that can be received by the switch CPU is limited to 1998 bytes, no matter what value was entered with the **system mtu** command. Although frames that are forwarded or routed typically are not received by the CPU, in some cases packets are sent to the CPU, such as traffic sent to control traffic, SNMP, Telnet, or routing protocols.

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

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
```

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

Related Commands

Command	Description
mpls mtu	Sets the MTU for MPLS labeled packets. The range is from 64 to 65536 bytes.
show system mtu	Displays the maximum packet size set for Fast Ethernet ports, Gigabit Ethernet ports, and routed ports.

traceroute mac

Use the **traceroute mac** privileged EXEC command to display the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address.

```
traceroute mac {[interface interface-id] {source-mac-address} [interface interface-id]
                 {destination-mac-address} [vlan vlan-id] [detail]}
```

Syntax Description		
interface <i>interface-id</i>	(Optional)	Specify an interface on the source or destination switch.
<i>source-mac-address</i>		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.
vlan <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 from 1 to 4094.
detail	(Optional)	Specify that detailed information appears.

Defaults There is no default.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on all the switches in the network. Do not disable CDP.

When the switch detects a device in the Layer 2 path that does not support Layer 2 traceroute, the switch continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

Layer 2 traceroute supports only unicast traffic. If you specify a multicast source or destination MAC address, the physical path is not identified, and an error message appears.

The **traceroute mac** command output shows the Layer 2 path when the specified source and destination addresses belong to the same VLAN. If you specify source and destination addresses that belong to different VLANs, the Layer 2 path is not identified, and an error message appears.

If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong. If the VLAN is not specified, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port). When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display the Layer 2 path by specifying the source and destination MAC addresses:

```
Switch# tracert mac 0000.0201.0601 0000.0201.0201

Source 0000.0201.0601 found on con6[ME-C3750-12TE] (2.2.6.6)
con6 (2.2.6.6) :Fa1/0/2 => Gi1/0/2
con5          (2.2.5.5) :      Gi1/0/2 => Fa1/0/2
con1          (2.2.1.1) :      Fa1/0/3 => Gi1/0/2
con2          (2.2.2.2) :      Fa1/0/2 => Fa0/0/3
Destination 0000.0201.0201 found on con2[ME-C3550-24TE] (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 0002.b3d3.bb29 0005.5d10.51d4 detail
Source 0002.b3d3.bb29 found on ip28-3750a[ME-C3750-24TE] (172.18.18.2)
1 ip28-3750a / ME-C3750-24TE / 172.18.18.2 :
      Gi1/1/1 [auto, 1000M] => Fa1/0/2 [auto, auto]
Destination 0005.5d10.51d4 found on ip28-3750a[ME-C3750-24TE] (172.18.18.2)
Layer2 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 fastethernet1/0/1 0000.0201.0601 interface
fastethernet1/0/3 0000.0201.0201
Source 0000.0201.0601 found on con6[ME-C3750-12TE] (2.2.6.6)
con6 (2.2.6.6) :Gi1/0/1 => Gi0/0/2
con5          (2.2.5.5) :      Gi1/0/2 => Gi0/0/1
con1          (2.2.1.1) :      Gi1/0/1 => Gi1/0/2
con2          (2.2.2.2) :      Gi1/0/2 => Gi1/0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

This example shows the Layer 2 path when the switch is not connected to the source switch:

```
Switch# tracert mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source ....
Source 0000.0201.0501 found on con5[ME-C3750-12TE] (2.2.5.5)
con5 / WS-C3750-12T / 2.2.5.5 :
      Gi1/0/1 [auto, auto] => Gi1/0/3 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
      Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
      Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows the Layer 2 path when the switch cannot find the destination port for the source MAC address:

```
Switch# tracert 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# tracert 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# tracert mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
```


This example shows the Layer 2 path when source and destination switches belong to multiple VLANs:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace aborted.
```

Related Commands	Command	Description
	traceroute mac ip	Displays the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname.

traceroute mac ip

Use the **traceroute mac ip** privileged EXEC command to display the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname.

traceroute mac ip {*source-ip-address* | *source-hostname*} {*destination-ip-address* | *destination-hostname*} [**detail**]

Syntax Description

<i>source-ip-address</i>	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.
detail	(Optional) Specify that detailed information appears.

Defaults

There is no default.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on all the switches in the network. Do not disable CDP.

When the switch detects an device in the Layer 2 path that does not support Layer 2 traceroute, the switch continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

The **traceroute mac ip** command output shows the Layer 2 path when the specified source and destination IP addresses are in the same subnet. When you specify the IP addresses, the switch uses Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.

- If an ARP entry exists for the specified IP address, the switch uses the associated MAC address and identifies the physical path.
- If an ARP entry does not exist, the switch sends an ARP query and tries to resolve the IP address. The IP addresses must be in the same subnet. If the IP address is not resolved, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port). When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display the Layer 2 path by specifying the source and destination IP addresses and by using the **detail** keyword:

```
Switch# traceroute mac ip 172.18.18.3 172.18.18.4 detail
Translating IP to mac .....
172.18.18.3 => 0002.b3d3.bb2a
172.18.18.4 => 0002.b3d3.bb29

Source 0002.b3d3.bb2a found on ip28-3750a[ME-C3750-24TE] (172.18.18.2)
1 ip28-3750a / ME-C3750-24TE / 172.18.18.2 :
      Gi1/0/1 [auto, auto] => Gi1/1/1 [auto, 1000M]
Destination 0002.b3d3.bb29 found on ip28-3750a[ME-C3750-24TE] (172.18.18.2)
Layer2 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) :Gi1/0/1 => Gi1/0/2
con5          (2.2.5.5)   ) :   Gi1/0/2 => Gi0/1
con1          (2.2.1.1)   ) :   Gi0/0/1 => Gi0/2
con2          (2.2.2.2)   ) :   Gi0/0/2 => Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
```

This example shows the Layer 2 path when ARP cannot associate the source IP address with the corresponding MAC address:

```
Switch# traceroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
```

Related Commands

Command	Description
shutdown	Displays the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address.

trust

Use the **trust** policy-map class configuration command to define a trust state for traffic classified through the **class** policy-map configuration command. Use the **no** form of this command to return to the default setting.

trust [**cos** | **dscp** | **ip-precedence**]

no trust [**cos** | **dscp** | **ip-precedence**]

Syntax Description	cos	(Optional) Classify an ingress packet by using the packet class of service (CoS) value. For an untagged packet, the port default CoS value is used.
	dscp	(Optional) Classify an ingress packet by using the packet Differentiated Services Code Point (DSCP) values (most significant 6 bits of 8-bit service-type field). For a non-IP packet, the packet CoS value is used if the packet is tagged. If the packet is untagged, the default port CoS value is used to map CoS to DSCP.
	ip-precedence	(Optional) Classify an ingress packet by using the packet IP-precedence value (most significant 3 bits of 8-bit service-type field). For a non-IP packet, the packet CoS value is used if the packet is tagged. If the packet is untagged, the port default CoS value is used to map CoS to DSCP.

Defaults The action is not trusted. If no keyword is specified when the command is entered, the default is **dscp**.

Command Modes Policy-map class configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines Use this command to distinguish the quality of service (QoS) trust behavior for certain traffic from other traffic. For example, inbound traffic with certain DSCP values can be trusted. You can configure a class map to match and trust the DSCP values in the inbound traffic.

Trust values set with this command supersede trust values set with the **mls qos trust** interface configuration command.

The **trust** command is not supported in a hierarchical policy map attached to an enhanced-services (ES) port.

If you specify **trust cos**, QoS uses the received or default port CoS value and the CoS-to-DSCP map to generate a DSCP value for the packet.

If you specify **trust dscp**, QoS uses the DSCP value from the ingress packet. For non-IP packets that are tagged, QoS uses the received CoS value; for non-IP packets that are untagged, QoS uses the default port CoS value. In either case, the DSCP value for the packet is derived from the CoS-to-DSCP map.

If you specify **trust ip-precedence**, QoS uses the IP precedence value from the ingress packet and the IP-precedence-to-DSCP map. For non-IP packets that are tagged, QoS uses the received CoS value; for non-IP packets that are untagged, QoS uses the default port CoS value. In either case, the DSCP for the packet is derived from the CoS-to-DSCP map.

When port trust policies are used with 802.1Q tunneling, all ports sharing the same tunnel VLAN must be configured with the same trust policy, and the ports involved must use the same DSCP-to-DSCP mutation map. For more information, see the “[mls qos dscp-mutation](#)” section on page 2-248, the “[mls qos map](#)” section on page 2-252, and the “[mls qos trust](#)” section on page 2-279.

For 802.1Q tunnels, the switch processes inbound traffic on a standard port according to the trusted setting applied to this port. For information about how the switch configures the inner and outer tags for packets sent over the enhanced-services (ES) trunk port, see the “[mls qos trust](#)” section on page 2-279.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Examples

This example shows how to define a port trust state to trust inbound DSCP values for traffic classified with *class1*:

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
```

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

Related Commands

Command	Description
class	Specifies the name of the class whose traffic policy you want to create or change.
police	Configures a single-rate ingress traffic policer for a class of traffic.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
set	Classifies IP traffic by setting a CoS, a DSCP, an IP precedence, or the multiprotocol label switching (MPLS) experimental (EXP) bits in the packet.
show policy-map	Displays QoS policy maps.

uddld (global configuration)

Use the **uddld** 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.

uddld { **aggressive** | **enable** | **message time** *message-timer-interval* }

no uddld { **aggressive** | **enable** | **message** }

Syntax Description

aggressive	Enable UDLD in aggressive mode on all fiber-optic ports.
enable	Enable UDLD in normal mode on all fiber-optic ports.
message time <i>message-timer-interval</i>	Configure the period of time between UDLD probe messages on interfaces that are in the advertisement phase and are detected to be bidirectional. The range is 1 to 90 seconds.

Defaults

UDLD is disabled on all interfaces.
The message timer is set at 60 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.
12.2(25)EY2	The range for message-timer-interval was changed from 7 to 90 seconds to 1 to 90 seconds.

Usage Guidelines

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD can detect unidirectional links due to misconnected ports on fiber-optic connections. In aggressive mode, UDLD also can detect unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected ports 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 only affects fiber-optic ports. Use the **uddld** interface configuration command to enable UDLD on other interface types.

You can use these commands to reset an interface shut down by UDLD:

- The **uddld 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 **udld port disable** 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 ports:

```
Switch(config)# udld enable
```

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

Related Commands

Command	Description
show udld	Displays UDLD administrative and operational status for all interfaces or the specified interface.
udld (interface configuration)	Enables UDLD on an individual interface or prevents a fiber-optic port from being enabled by the udld global configuration command.
udld reset	Resets all interfaces shut down by UDLD and permits traffic to again pass through.

udld (interface configuration)

Use the **udld** interface configuration command to enable the UniDirectional Link Detection (UDLD) on an individual interface or prevent a fiber-optic port 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 on a nonfiber-optic port.

udld port {aggressive | disable}

no udld port {aggressive | disable}

Syntax Description

aggressive	Enable UDLD in aggressive mode on the specified interface.
disable	Disable UDLD on the specified interface. This keyword applies only to fiber-optic ports.

Defaults

On fiber-optic ports, UDLD is not enabled, in aggressive mode, or disabled. For this reason, fiber-optic ports enable UDLD according to the state of the **udld enable** or **udld aggressive** global configuration command.

On nonfiber-optic ports, UDLD is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

A UDLD-capable interface cannot detect a unidirectional link if it is connected to a UDLD-incapable interface of another switch.

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD can detect unidirectional links due to misconnected ports on fiber-optic connections. In aggressive mode, UDLD also can detect unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected ports 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.

The **disable** keyword is only supported on fiber-optic ports. Use the **no** form of this command to remove this setting and to return control of UDLD to the **udld** global configuration command.

If the switch software detects a Gigabit Interface Converter (GBIC) module change and the interface 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 **udld port disable** 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 a port:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# udld port
```

This example shows how to disable UDLD on a fiber-optic port despite the setting of the **udld** global configuration command:

```
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# udld port disable
```

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

Related Commands

Command	Description
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.
show udld	Displays UDLD administrative and operational status for all interfaces or the specified interface.
udld (global configuration)	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
udld reset	Resets all interfaces shut down by UDLD and permits traffic to again pass through.

uddl reset

Use the **uddl reset** privileged EXEC command to reset all interfaces disabled by the UniDirectional Link Detection (UDLD) and permit traffic to begin passing through them again (though other features, such as spanning tree, Port Aggregation Protocol (PAgP), and Dynamic Trunking Protocol (DTP) still have their normal effects, if enabled).

uddl reset

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines If the interface configuration is still enabled for UDLD, these interfaces 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# uddl reset
1 ports shutdown by UDLD were reset.
```

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

Related Commands	Command	Description
	show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.
	show uddl	Displays UDLD administrative and operational status for all interfaces or the specified interface.
	uddl (global configuration)	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
	uddl (interface configuration)	Enables UDLD on an individual interface or prevents a fiber-optic port from being enabled by the uddl 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.
multipoint	(Optional) Select point-to-multipoint service. This keyword is visible only when you enter a uni count value of 2. - 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. - If you enter a uni count value of 3 or greater, the service is point-to-multipoint.

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(25)SEG	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-evc)# uni count 2 multipoint
```

Related Commands

Command	Description
ethernet evc <i>evc-id</i>	Defines an EVC and enters EVC configuration mode.

vlan (global configuration)

Use the **vlan** global configuration command to add a VLAN and to enter the config-vlan mode. Use the **no** form of this command to delete the VLAN. Configuration information for normal-range VLANs (VLAN IDs 1 to 1005) is always saved in the VLAN database. When VLAN Trunking Protocol (VTP) mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005), and the VTP mode, domain name, and the VLAN configuration are saved in the switch running configuration file. You can save configurations in the switch startup configuration file by entering the **copy running-config startup-config** privileged EXEC command.

vlan *vlan-id*

no vlan *vlan-id*

Syntax Description	<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
	12.1(14)AX	This command was introduced.

Usage Guidelines	You must use the vlan <i>vlan-id</i> global configuration command to add extended-range VLANs (VLAN IDs 1006 to 4094). Before configuring VLANs in the extended range, you must use the vtp transparent global configuration or VLAN configuration command to put the switch in VTP transparent mode. Extended-range VLANs are not learned by VTP and are not added to the VLAN database, but when VTP mode is transparent, VTP mode and domain name and all VLAN configurations are saved in the running configuration, and you can save them in the switch startup configuration file.

When you save the VLAN and VTP configurations in the startup configuration file and reboot the switch, the configuration is determined in these ways:

- If both the VLAN database and the configuration file show the VTP mode as transparent and the VTP domain names match, the VLAN database is ignored. The VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode is server, or if the startup VTP mode or domain names do not match the VLAN database, the VTP mode and the VLAN configuration for the first 1005 VLANs use the VLAN database information.

If you try to create an extended-range VLAN when the switch is not in VTP transparent mode, the VLAN is rejected, and you receive an error message.

If you enter an invalid VLAN ID, you receive an error message and do not enter config-vlan mode.

Entering the **vlan** command with a VLAN ID enables config-vlan mode. When you enter the VLAN ID of an existing VLAN, you do not create a new VLAN, but you can modify VLAN parameters for that VLAN. The specified VLANs are added or modified when you exit the config-vlan mode. Only the **shutdown** command (for VLANs 1 to 1005) takes effect immediately.

These configuration commands are available in config-vlan mode. The **no** form of each command returns the characteristic to its default state.

**Note**

Although all commands are visible, the only config-vlan command supported on extended-range VLANs is **mtu mtu-size**. For extended-range VLANs, all other characteristics must remain at the default state.

- **are are-number**: defines the maximum number of all-routes explorer (ARE) hops for this VLAN. This keyword applies only to TrCRF VLANs. The range is 0 to 13. The default is 7. If no value is entered, 0 is assumed to be the maximum.
- **backupcrf**: specifies the backup CRF mode. This keyword applies only to TrCRF VLANs.
 - **enable** backup CRF mode for this VLAN.
 - **disable** backup CRF mode for this VLAN (the default).
- **bridge {bridge-number| type}**: specifies the logical distributed source-routing bridge, the bridge that interconnects all logical rings having this VLAN as a parent VLAN in FDDI-NET, Token Ring-NET, and TrBRF VLANs. The range is 0 to 15. The default bridge number is 0 (no source-routing bridge) for FDDI-NET, TrBRF, and Token Ring-NET VLANs. The **type** keyword applies only to TrCRF VLANs and is one of these:
 - **srb** (source-route bridging)
 - **srt** (source-route transparent) bridging VLAN
- **exit**: applies changes, increments the VLAN database revision number (VLANs 1 to 1005 only), and exits config-vlan mode.
- **media**: defines the VLAN media type. See [Table 2-34](#) for valid commands and syntax for different media types.

**Note**

The switch supports only Ethernet ports. You configure only FDDI and Token Ring media-specific characteristics for VLAN Trunking Protocol (VTP) global advertisements to other switches. These VLANs are locally suspended.

- **ethernet** is Ethernet media type (the default).
- **fddi** is FDDI media type.
- **fd-net** is FDDI network entity title (NET) media type.
- **tokenring** is Token Ring media type if the VTP v2 mode is disabled, or TrCRF if the VTP version 2 (v) mode is enabled.
- **tr-net** is Token Ring network entity title (NET) media type if the VTP v2 mode is disabled or TrBRF media type if the VTP v2 mode is enabled.
- **mtu mtu-size**: specifies the maximum transmission unit (MTU) (packet size in bytes). The range is 1500 to 18190. The default is 1500 bytes.

- **name** *vlan-name*: names the VLAN with an ASCII string from 1 to 32 characters that must be unique within the administrative domain. The default is *VLANxxxx* where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number.
- **no**: negates a command or returns it to the default setting.
- **parent** *parent-vlan-id*: specifies the parent VLAN of an existing FDDI, Token Ring, or TrCRF VLAN. This parameter identifies the TrBRF to which a TrCRF belongs and is required when defining a TrCRF. The range is 0 to 1005. The default parent VLAN ID is 0 (no parent VLAN) for FDDI and Token Ring VLANs. For both Token Ring and TrCRF VLANs, the parent VLAN ID must already exist in the database and be associated with a Token Ring-NET or TrBRF VLAN.

**Note**

Though visible in the command-line interface, the **private-vlan** command is not supported.

- **remote-span**: configure the VLAN as a Remote SPAN (RSPAN) VLAN. When the RSPAN feature is added to an existing VLAN, the VLAN is first deleted and is then recreated with the RSPAN feature. Any access ports are deactivated until the RSPAN feature is removed. If VTP is enabled, the new RSPAN VLAN is propagated by VTP for VLAN-IDs that are lower than 1024. Learning is disabled on the VLAN. 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. The default for Token Ring VLANs is 0. For FDDI VLANs, there is no default.
- **said** *said-value*: specifies the security association identifier (SAID) as documented in IEEE 802.10. The range is 1 to 4294967294, and the number must be unique within the administrative domain. The default value is 100000 plus the VLAN ID number.
- **shutdown**: shuts down VLAN switching on the VLAN. This command takes effect immediately. Other commands take effect when you exit config-vlan mode.
- **state**: specifies the VLAN state:
 - **active** means the VLAN is operational (the default).
 - **suspend** means the VLAN is suspended. Suspended VLANs do not pass packets.
- **ste** *ste-number*: defines the maximum number of spanning-tree explorer (STE) hops. This keyword applies only to TrCRF VLANs. The range is 0 to 13. The default is 7.
- **stp type**: defines the spanning-tree type for FDDI-NET, Token Ring-NET, or TrBRF VLANs. For FDDI-NET VLANs, the default STP type is **ieee**. For Token Ring-NET VLANs, the default STP type is **ibm**. For FDDI and Token Ring VLANs, the default is no type specified.
 - **ieee** for IEEE Ethernet STP running source-route transparent (SRT) bridging.
 - **ibm** for IBM STP running source-route bridging (SRB).
 - **auto** for STP running a combination of source-route transparent bridging (IEEE) and source-route bridging (IBM).
- **tb-vlan1** *tb-vlan1-id* and **tb-vlan2** *tb-vlan2-id*: specifies the first and second VLAN to which this VLAN is translationally bridged. Translational VLANs translate FDDI or Token Ring to Ethernet, for example. The range is 0 to 1005. If no value is specified, 0 (no transitional bridging) is assumed.

Table 2-34 Valid Commands and Syntax for Different Media Types

Media Type	Valid Syntax
Ethernet	name <i>vlan-name</i> , media ethernet, state {suspend active}, said <i>said-value</i> , mtu <i>mtu-size</i> , remote-span , tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>
FDDI	name <i>vlan-name</i> , media fddi, state {suspend active}, said <i>said-value</i> , mtu <i>mtu-size</i> , ring <i>ring-number</i> , parent <i>parent-vlan-id</i> , tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>
FDDI-NET	name <i>vlan-name</i> , media fd-net, state {suspend active}, said <i>said-value</i> , mtu <i>mtu-size</i> , bridge <i>bridge-number</i> , stp type {ieee ibm auto}, tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i> If VTP v2 mode is disabled, do not set the stp type to auto.
Token Ring	VTP v1 mode is enabled. name <i>vlan-name</i> , media tokenring, state {suspend active}, said <i>said-value</i> , mtu <i>mtu-size</i> , ring <i>ring-number</i> , parent <i>parent-vlan-id</i> , tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>
Token Ring concentrator relay function (TrCRF)	VTP v2 mode is enabled. name <i>vlan-name</i> , media tokenring, state {suspend active}, said <i>said-value</i> , mtu <i>mtu-size</i> , ring <i>ring-number</i> , parent <i>parent-vlan-id</i> , bridge type {srb srt}, are <i>are-number</i> , ste <i>ste-number</i> , backupcrf {enable disable}, tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>
Token Ring-NET	VTP v1 mode is enabled. name <i>vlan-name</i> , media tr-net, state {suspend active}, said <i>said-value</i> , mtu <i>mtu-size</i> , bridge <i>bridge-number</i> , stp type {ieee ibm}, tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>
Token Ring bridge relay function (TrBRF)	VTP v2 mode is enabled. name <i>vlan-name</i> , media tr-net, state {suspend active}, said <i>said-value</i> , mtu <i>mtu-size</i> , bridge <i>bridge-number</i> , stp type {ieee ibm auto}, tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>

Table 2-35 describes the rules for configuring VLANs.

Table 2-35 VLAN Configuration Rules

Configuration	Rule
VTP v2 mode is enabled, and you are configuring a TrCRF VLAN media type.	Specify a parent VLAN ID of a TrBRF that already exists in the database. Specify a ring number. Do not leave this field blank. Specify unique ring numbers when TrCRF VLANs have the same parent VLAN ID. Only one backup concentrator relay function (CRF) can be enabled.
VTP v2 mode is enabled, and you are configuring VLANs other than TrCRF media type.	Do not specify a backup CRF.

Table 2-35 VLAN Configuration Rules (continued)

Configuration	Rule
VTP v2 mode is enabled, and you are configuring a TrBRF VLAN media type.	Specify a bridge number. Do not leave this field blank.
VTP v1 mode is enabled.	No VLAN can have an STP type set to auto. This rule applies to Ethernet, FDDI, FDDI-NET, Token Ring, and Token Ring-NET VLANs.
Add a VLAN that requires translational bridging (values are not set to zero).	The translational bridging VLAN IDs that are used must already exist in the database. The translational bridging VLAN IDs that a configuration points to must also contain a pointer to the original VLAN in one of the translational bridging parameters (for example, Ethernet points to FDDI, and FDDI points to Ethernet). The translational bridging VLAN IDs that a configuration points to must be different media types than the original VLAN (for example, Ethernet can point to Token Ring). If both translational bridging VLAN IDs are configured, these VLANs must be different media types (for example, Ethernet can point to FDDI and Token Ring).

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** config-vlan configuration command, the VLAN is added if it did not already exist; otherwise, this command does nothing.

This example shows how to create a new VLAN with all default characteristics and enter config-vlan mode:

```
Switch(config)# vlan 200
Switch(config-vlan)# exit
Switch(config)#
```

This example shows how to create a new extended-range VLAN with all the default characteristics, to enter config-vlan mode, and to save the new VLAN in the switch startup configuration file:

```
Switch(config)# vtp mode transparent
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config
```

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

Related Commands	Command	Description
	show sdm prefer	Displays all or a range of VLAN-related configurations on the switch.
	show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) in the administrative domain.
	vlan (VLAN configuration)	Configures normal-range VLANs in the VLAN database.

vlan (VLAN configuration)

Use the **vlan** VLAN configuration command to configure VLAN characteristics for a normal-range VLAN (VLAN IDs 1 to 1005) in the VLAN database. You access VLAN configuration mode by entering the **vlan database** privileged EXEC command. Use the **no** form of this command without additional parameters to delete a VLAN. Use the **no** form with parameters to change its configured characteristics.

```

vlan vlan-id [are are-number] [backupcrf {enable | disable}] [bridge bridge-number |
type {srb | srt}] [media {ethernet | fddi | fdi-net | tokenring | tr-net}] [mtu mtu-size]
[name vlan-name] [parent parent-vlan-id] [ring ring-number] [said said-value]
[state {suspend | active}] [ste ste-number] [stp type {ieee | ibm | auto}]
[tb-vlan1 tb-vlan1-id] [tb-vlan2 tb-vlan2-id]

```

```

no vlan vlan-id [are are-number] [backupcrf {enable | disable}] [bridge bridge-number |
type {srb | srt}] [media {ethernet | fddi | fdi-net | tokenring | tr-net}] [mtu mtu-size]
[name vlan-name] [parent parent-vlan-id] [ring ring-number] [said said-value]
[state {suspend | active}] [ste ste-number] [stp type {ieee | ibm | auto}]
[tb-vlan1 tb-vlan1-id] [tb-vlan2 tb-vlan2-id]

```

Extended-range VLANs (with VLAN IDs from 1006 to 4094) cannot be added or modified by using these commands. To add extended-range VLANs, use the **vlan (global configuration)** command to enter config-vlan mode.



Note

The switch supports only Ethernet ports. You configure only FDDI and Token Ring media-specific characteristics for VLAN Trunking Protocol (VTP) global advertisements to other switches. These VLANs are locally suspended.

Syntax Description

<i>vlan-id</i>	ID of the configured VLAN. The range is 1 to 1005 and must be unique within the administrative domain. Do not enter leading zeros.
are <i>are-number</i>	(Optional) Specify the maximum number of all-routes explorer (ARE) hops for this VLAN. This keyword applies only to TrCRF VLANs. The range is 0 to 13. If no value is entered, 0 is assumed to be the maximum.
backupcrf { enable disable }	(Optional) Specify the backup CRF mode. This keyword applies only to TrCRF VLANs. enable backup CRF mode for this VLAN. disable backup CRF mode for this VLAN.
bridge <i>bridge-number</i> type { srb srt }	(Optional) Specify 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 type keyword applies only to TrCRF VLANs and is one of these: srb (source-route bridging) srt (source-route transparent) bridging VLAN

media { ethernet fddi fd-net tokenring tr-net }	(Optional) Specify the VLAN media type. Table 2-36 lists the valid syntax for each 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 if the VTP v2 mode is disabled, or TrCRF if the VTP v2 mode is enabled. • tr-net is Token Ring network entity title (NET) media type if the VTP v2 mode is disabled or TrBRF media type if the VTP v2 mode is enabled.
mtu <i>mtu-size</i>	(Optional) Specify the maximum transmission unit (MTU) (packet size in bytes). The range is 1500 to 18190.
name <i>vlan-name</i>	(Optional) Specify the VLAN name, an ASCII string from 1 to 32 characters that must be unique within the administrative domain.
parent <i>parent-vlan-id</i>	(Optional) Specify the parent VLAN of an existing FDDI, Token Ring, or TrCRF VLAN. This parameter identifies the TrBRF to which a TrCRF belongs and is required when defining a TrCRF. The range is 0 to 1005.
ring <i>ring-number</i>	(Optional) Specify the logical ring for an FDDI, Token Ring, or TrCRF VLAN. The range is 1 to 4095.
said <i>said-value</i>	(Optional) Enter 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.
state { suspend active }	(Optional) Specify the VLAN state: • If active, the VLAN is operational. • If suspend, the VLAN is suspended. Suspended VLANs do not pass packets.
ste <i>ste-number</i>	(Optional) Specify the maximum number of spanning-tree explorer (STE) hops. This keyword applies only to TrCRF VLANs. The range is 0 to 13.
stp type { ieee ibm auto }	(Optional) Specify the spanning-tree type for FDDI-NET, Token Ring-NET, or TrBRF VLAN. • 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 <i>tb-vlan1-id</i> and tb-vlan2 <i>tb-vlan2-id</i>	(Optional) Specify 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. Zero is assumed if no value is specified.

Table 2-36 shows the valid syntax options for different media types.

Table 2-36 Valid Syntax for Different Media Types

Media Type	Valid Syntax
Ethernet	vlan <i>vlan-id</i> [name <i>vlan-name</i>] media ethernet [state { suspend active }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>]
FDDI	vlan <i>vlan-id</i> [name <i>vlan-name</i>] media fddi [state { suspend active }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [ring <i>ring-number</i>] [parent <i>parent-vlan-id</i>] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>]
FDDI-NET	vlan <i>vlan-id</i> [name <i>vlan-name</i>] media fd-net [state { suspend active }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [bridge <i>bridge-number</i>] [stp type { ieee ibm auto }] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>] If VTP v2 mode is disabled, do not set the stp type to auto .
Token Ring	VTP v1 mode is enabled. vlan <i>vlan-id</i> [name <i>vlan-name</i>] media tokenring [state { suspend active }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [ring <i>ring-number</i>] [parent <i>parent-vlan-id</i>] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>]
Token Ring concentrator relay function (TrCRF)	VTP v2 mode is enabled. vlan <i>vlan-id</i> [name <i>vlan-name</i>] media tokenring [state { suspend active }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [ring <i>ring-number</i>] [parent <i>parent-vlan-id</i>] [bridge type { srb srt }] [are <i>are-number</i>] [ste <i>ste-number</i>] [backupcrf { enable disable }] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>]
Token Ring-NET	VTP v1 mode is enabled. vlan <i>vlan-id</i> [name <i>vlan-name</i>] media tr-net [state { suspend active }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [bridge <i>bridge-number</i>] [stp type { ieee ibm }] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>]
Token Ring bridge relay function (TrBRF)	VTP v2 mode is enabled. vlan <i>vlan-id</i> [name <i>vlan-name</i>] media tr-net [state { suspend active }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [bridge <i>bridge-number</i>] [stp type { ieee ibm auto }] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>]

Table 2-37 describes the rules for configuring VLANs.

Table 2-37 VLAN Configuration Rules

Configuration	Rule
VTP v2 mode is enabled, and you are configuring a TrCRF VLAN media type.	Specify a parent VLAN ID of a TrBRF that already exists in the database. Specify a ring number. Do not leave this field blank. Specify unique ring numbers when TrCRF VLANs have the same parent VLAN ID. Only one backup concentrator relay function (CRF) can be enabled.
VTP v2 mode is enabled, and you are configuring VLANs other than TrCRF media type.	Do not specify a backup CRF.

Table 2-37 VLAN Configuration Rules (continued)

Configuration	Rule
VTP v2 mode is enabled, and you are configuring a TrBRF VLAN media type.	Specify a bridge number. Do not leave this field blank.
VTP v1 mode is enabled.	No VLAN can have an STP type set to auto. This rule applies to Ethernet, FDDI, FDDI-NET, Token Ring, and Token Ring-NET VLANs.
Add a VLAN that requires translational bridging (values are not set to zero).	The translational bridging VLAN IDs that are used must already exist in the database. The translational bridging VLAN IDs that a configuration points to must also contain a pointer to the original VLAN in one of the translational bridging parameters (for example, Ethernet points to FDDI, and FDDI points to Ethernet). The translational bridging VLAN IDs that a configuration points to must be different media types than the original VLAN (for example, Ethernet can point to Token Ring). If both translational bridging VLAN IDs are configured, these VLANs must be different media types (for example, Ethernet can point to FDDI and Token Ring).

Defaults

The ARE value is 7.

Backup CRF is disabled.

The bridge number is 0 (no source-routing bridge) for FDDI-NET, TrBRF, and Token Ring-NET VLANs.

The **media** type is **ethernet**.

The default *mtu size* is 1500 bytes.

The *vlan-name* variable is *VLANxxxx*, where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number.

The parent VLAN ID is 0 (no parent VLAN) for FDDI and Token Ring VLANs. For TrCRF VLANs, you must specify a parent VLAN ID. For both Token Ring and TrCRF VLANs, the parent VLAN ID must already exist in the database and be associated with a Token Ring-NET or TrBRF VLAN.

The *ring number* for Token Ring VLANs is 0. For FDDI VLANs, there is no default.

The *said value* is 100000 plus the VLAN ID.

The state is **active**.

The STE value is 7.

The STP type is **ieee** for FDDI-NET and **ibm** for Token Ring-NET VLANs. For FDDI and Token Ring VLANs, the default is no type specified.

The *tb-vlan1-id* and *tb-vlan2-id* variables are zero (no translational bridging).

Command Modes

VLAN configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

You can only use this command mode for configuring normal-range VLANs, that is, VLAN IDs 1 to 1005.

**Note**

To configure extended-range VLANs (VLAN IDs 1006 to 4094), use the **vlan** global configuration command.

VLAN configuration is always saved in the VLAN database. If VTP mode is transparent, it is also saved in the switch running configuration file, along with the VTP mode and domain name. You can then save it in the switch startup configuration file by using the **copy running-config startup-config** privileged EXEC command.

When you save VLAN and VTP configuration in the startup configuration file and reboot the switch, the configuration is determined in these ways:

- If both the VLAN database and the configuration file show the VTP mode as transparent and the VTP domain names match, the VLAN database is ignored. The VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode is server, or if the startup VTP mode or domain names do not match the VLAN database, the VTP mode and the VLAN configuration for the first 1005 VLANs use VLAN database information.

The following are the results of using the **no vlan** commands:

- When the **no vlan vlan-id** form is used, the VLAN is deleted. Deleting VLANs automatically resets to zero any other parent VLANs and translational bridging parameters that refer to the deleted VLAN.
- When the **no vlan vlan-id bridge** form is used, the VLAN source-routing bridge number returns to the default (0). The **vlan vlan-id bridge** command is used only for FDDI-NET and Token Ring-NET VLANs and is ignored in other VLAN types.
- When the **no vlan vlan-id media** form is used, the media type returns to the default (**ethernet**). Changing the VLAN media type (including the **no** form) resets the VLAN MTU to the default MTU for the type (unless the **mtu** keyword is also present in the command). It also resets the VLAN parent and translational bridging VLAN to the default (unless the **parent**, **tb-vlan1**, or **tb-vlan2** are also present in the command).
- When the **no vlan vlan-id mtu** form is used, the VLAN MTU returns to the default for the applicable VLAN media type. You can also modify the MTU by using the **media** keyword.
- When the **no vlan vlan-id name vlan-name** form is used, the VLAN name returns to the default name (VLANxxxx, where xxxx represent four numeric digits [including leading zeros] equal to the VLAN ID number).
- When the **no vlan vlan-id parent** form is used, the parent VLAN returns to the default (0). The parent VLAN resets to the default if the parent VLAN is deleted or if the **media** keyword changes the VLAN type or the VLAN type of the parent VLAN.
- When the **no vlan vlan-id ring** form is used, the VLAN logical ring number returns to the default (0).

- When the **no vlan *vlan-id* said** form is used, the VLAN SAID returns to the default (100,000 plus the VLAN ID).
- When the **no vlan *vlan-id* state** form is used, the VLAN state returns to the default (**active**).
- When the **no vlan *vlan-id* stp type** form is used, the VLAN spanning-tree type returns to the default (**ieee**).
- When the **no vlan *vlan-id* tb-vlan1** or **no vlan *vlan-id* tb-vlan2** form is used, the VLAN translational bridge VLAN (or VLANs, if applicable) returns to the default (0). Translational bridge VLANs must be a different VLAN type than the affected VLAN, and if two are specified, the two must be different VLAN types from each other. A translational bridge VLAN resets to the default if the translational bridge VLAN is deleted, if the **media** keyword changes the VLAN type, or if the **media** keyword changes the VLAN type of the corresponding translation bridge VLAN.

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** or **apply** vlan configuration command, the VLAN is added if it did not already exist; otherwise, this command does nothing.

```
Switch(vlan)# vlan 2
VLAN 2 added:
    Name: VLAN0002
Switch(vlan)# exit
APPLY completed.
Exiting....
```

This example shows how to modify an existing VLAN by changing its name and MTU size:

```
Switch(vlan)# no vlan name engineering mtu 1200
```

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

Related Commands

Command	Description
show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) in the administrative domain.
vlan (global configuration)	Enters config-vlan mode for configuring normal-range and extended-range VLANs.

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
	12.1(14)AX	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.

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 ac11  
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
action	Sets the action for the VLAN access map entry.
match (access-map configuration)	Sets the VLAN map to match packets against one or more access lists.
show vlan access-map	Displays information about a particular VLAN access map or all VLAN access maps.
vlan filter	Applies the VLAN access map to one or more VLANs.

vlan database

Use the **vlan database** privileged EXEC command to enter VLAN configuration mode. From this mode, you can add, delete, and modify VLAN configurations for normal-range VLANs and globally propagate these changes by using the VLAN Trunking Protocol (VTP). Configuration information is saved in the VLAN database.

vlan database

**Note**

VLAN configuration mode is only valid for VLAN IDs 1 to 1005.

Syntax Description

This command has no arguments or keywords.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

You can use the VLAN database configuration commands to configure VLANs 1 to 1005. To configure extended-range VLANs (VLAN IDs 1006 to 4094), use the **vlan (global configuration)** command to enter config-vlan mode. You can also configure VLAN IDs 1 to 1005 by using the **vlan** global configuration command.

To return to the privileged EXEC mode from the VLAN configuration mode, enter the **exit** command.

**Note**

This command mode is different from other modes because it is session-oriented. When you add, delete, or modify VLAN parameters, the changes are not applied until you exit the session by entering the **apply** or **exit** command. When the changes are applied, the VTP configuration version is incremented. You can also *not* apply the changes to the VTP database by entering **abort**.

When you are in VLAN configuration mode, you can access the VLAN database and make changes by using these commands:

- **vlan**: accesses subcommands to add, delete, or modify values associated with a single VLAN. For more information, see the **vlan (VLAN configuration)** command.
- **vtp**: accesses subcommands to perform VTP administrative functions. For more information, see the **vtp (VLAN configuration)** command.

When you have modified VLAN or VTP parameters, you can use these editing buffer manipulation commands:

- **abort**: exits the mode without applying the changes. The VLAN configuration that was running before you entered VLAN configuration mode continues to be used.
- **apply**: applies current changes to the VLAN database, increments the database configuration revision number, propagates it throughout the administrative domain, and remains in VLAN configuration mode.



Note You cannot use this command when the switch is in VTP client mode.

- **exit**: applies all configuration changes to the VLAN database, increments the database configuration number, propagates it throughout the administrative domain, and returns to privileged EXEC mode.
- **no**: negates a command or set its defaults; valid values are **vlan** and **vtp**.
- **reset**: abandons proposed changes to the VLAN database, resets the proposed database to the implemented VLAN database on the switch, and remains in VLAN configuration mode.
- **show**: displays VLAN database information.
- **show changes** [*vlan-id*]: displays the differences between the VLAN database on the switch and the proposed VLAN database for all normal-range VLAN IDs (1 to 1005) or the specified VLAN ID (1 to 1005).
- **show current** [*vlan-id*]: displays the VLAN database on the switch or on a selected VLAN (1 to 1005).
- **show proposed** [*vlan-id*]: displays the proposed VLAN database or a selected VLAN (1 to 1005) from the proposed database. The proposed VLAN database is not the running configuration until you use the **exit** or **apply** VLAN configuration command.

You can verify that VLAN database changes have been made or aborted by using the **show vlan** privileged EXEC command. This output is different from the **show** VLAN database configuration command output.

Examples

This example shows how to enter the VLAN configuration mode from the privileged EXEC mode and to display VLAN database information:

```
Switch# vlan database
Switch(vlan)# show
VLAN ISL Id: 1
  Name: default
  Media Type: Ethernet
VLAN 802.10 Id: 100001
  State: Operational
  MTU: 1500
  Translational Bridged VLAN: 1002
  Translational Bridged VLAN: 1003

VLAN ISL Id: 2
  Name: VLAN0002
  Media Type: Ethernet
VLAN 802.10 Id: 100002
  State: Operational
  MTU: 1500

VLAN ISL Id: 1002
  Name: fddi-default
```

```
Media Type: FDDI
VLAN 802.10 Id: 101002
State: Operational
MTU: 1500
Bridge Type: SRB
Ring Number: 0
Translational Bridged VLAN: 1
Translational Bridged VLAN: 1003
```

<output truncated>

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

```
Switch(vlan)# show changes
```

```
DELETED:
  VLAN ISL Id: 4
    Name: VLAN0004
    Media Type: Ethernet
    VLAN 802.10 Id: 100004
    State: Operational
    MTU: 1500

MODIFIED:
  VLAN ISL Id: 7
    Current State: Operational
    Modified State: Suspended
```

This example shows how to display the differences between VLAN 7 in the current database and the proposed database:

```
Switch(vlan)# show changes 7
```

```
MODIFIED:
  VLAN ISL Id: 7
    Current State: Operational
    Modified State: Suspended
```

This is an example of output from the **show current 20** command. It displays only VLAN 20 of the current database:

```
Switch(vlan)# show current 20
VLAN ISL Id: 20
  Name: VLAN0020
  Media Type: Ethernet
  VLAN 802.10 Id: 100020
  State: Operational
  MTU: 1500
```

Related Commands	Command	Description
	show vlan	Displays the parameters for all configured VLANs in the administrative domain.
	shutdown vlan	Shuts down (suspends) local traffic on the specified VLAN.
	vlan (global configuration)	Enters config-vlan mode for configuring normal-range and extended-range VLANs.

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.
all	Remove the filter from all VLANs.

Defaults

There are no VLAN filters.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

To avoid accidentally dropping too many packets and disabling connectivity in the middle of the configuration process, we recommend that you completely define the VLAN access map before applying it to a VLAN.

For more information about VLAN map entries, see the software configuration guide for this release.

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
	show vlan access-map	Displays information about a particular VLAN access map or all VLAN access maps.
	show vlan filter	Displays information about all VLAN filters or about a particular VLAN or VLAN access map.
	vlan access-map	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
	12.1(14)AX	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
	show vmps	Displays VQP and VMPS information.
	vmps reconfirm (global configuration)	Changes the reconfirmation interval for the VLAN Query Protocol (VQP) client.

vmmps reconfirm (global configuration)

Use the **vmmps 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.

vmmps reconfirm *interval*

no vmmps reconfirm

Syntax Description	<i>interval</i>	Reconfirmation interval for VQP client queries to the VLAN Membership Policy Server (VMPS) to reconfirm dynamic VLAN assignments. The range is 1 to 120 minutes.

Defaults	The default reconfirmation interval is 60 minutes.

Command Modes	Global configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Examples	This example shows how to set the VQP client to reconfirm dynamic VLAN entries every 20 minutes:

```
Switch(config)# vmmps reconfirm 20
```

You can verify your setting by entering the **show vmmps** privileged EXEC command and examining information in the Reconfirm Interval row.

Related Commands	Command	Description
	show vmmps	Displays VQP and VMPS information.
	vmmps reconfirm (privileged EXEC)	Sends VQP queries to reconfirm all dynamic VLAN assignments with the VMPS.

vmpls retry

Use the **vmpls 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.

vmpls retry *count*

no vmpls retry

Syntax Description	<i>count</i>	Number of attempts to contact the VLAN Membership Policy Server (VMPS) by the client before querying the next server in the list. The range is 1 to 10.

Defaults	The default retry count is 3.

Command Modes	Global configuration

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Examples	This example shows how to set the retry count to 7:

```
Switch(config)# vmpls retry 7
```

You can verify your setting by entering the **show vmpls** privileged EXEC command and examining information in the Server Retry Count row.

Related Commands	Command	Description
	show vmpls	Displays VQP and VMPS information.

vmips server

Use the **vmips 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.

vmips server *ipaddress* [**primary**]

no vmips 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.
primary	(Optional) Determines 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
12.1(14)AX	This command was introduced.

Usage Guidelines

The first server entered is automatically selected as the primary server whether or not **primary** is entered. The first server address can be overridden by using **primary** in a subsequent command.

If a member switch in a cluster configuration does not have an IP address, the cluster does not use the VMPS server configured for that member switch. Instead, the cluster uses the VMPS server on the command switch, and the command switch proxies the VMPS requests. The VMPS server treats the cluster as a single switch and uses the IP address of the command switch to respond to requests.

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 with IP address 191.10.49.20 as the primary VMPS server. The servers with IP addresses 191.10.49.21 and 191.10.49.22 are configured as secondary servers.

```
Switch(config)# vmips server 191.10.49.20 primary  
Switch(config)# vmips server 191.10.49.21  
Switch(config)# vmips server 191.10.49.22
```

This example shows how to delete the server with IP address 191.10.49.21:

```
Switch(config)# no vmips server 191.10.49.21
```

You can verify your setting by entering the **show vmps** privileged EXEC command and examining information in the VMPS Domain Server row.

Related Commands	Command	Description
	show vmps	Displays VQP and VMPS information.

vtp (global configuration)

Use the **vtp** global configuration command to set or modify the VLAN Trunking Protocol (VTP) configuration characteristics. Use the **no** form of this command to remove the settings or to return to the default settings.

vtp {**domain** *domain-name* | **file** *filename* | **interface** *name* [**only**] | **mode** {**client** | **server** | **transparent**} | **password** *password* | **pruning** | **version** *number*}

no vtp {**file** | **interface** | **mode** | **password** | **pruning** | **version**}

Syntax Description	
domain <i>domain-name</i>	Specify the VTP domain name, an ASCII string from 1 to 32 characters that identifies the VTP administrative domain for the switch. The domain name is case sensitive.
file <i>filename</i>	Specify the Cisco IOS file system file where the VTP VLAN configuration is stored.
interface <i>name</i>	Specify the name of the interface providing the VTP ID updated for this device.
only	(Optional) Use only the IP address of this interface as the VTP IP updater.
mode	Specify the VTP device mode as client, server, or transparent.
client	Place the switch in VTP client mode. A switch in VTP client mode is enabled for VTP, and can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on the switch. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database.
server	Place the switch in VTP server mode. A switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on the switch. The switch can recover all the VLAN information in the current VTP database from nonvolatile storage after reboot.
transparent	Place the switch in VTP transparent mode. A switch in VTP transparent mode is disabled for VTP, does not send advertisements or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The switch receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received. When VTP mode is transparent, the mode and domain name are saved in the switch running configuration file, and you can save them in the switch startup configuration file by entering the copy running-config startup config privileged EXEC command.
password <i>password</i>	Set the administrative domain password for the generation of the 16-byte secret value used in MD5 digest calculation to be sent in VTP advertisements and to validate received VTP advertisements. The password can be an ASCII string from 1 to 32 characters. The password is case sensitive.
pruning	Enable VTP pruning on the switch.
version <i>number</i>	Set VTP version to version 1 or version 2.

Defaults

The default filename is *flash:vlan.dat*.

The default mode is server mode.

No domain name or password is defined.

No password is configured.

Pruning is disabled.

The default version is version 1.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

When you save VTP mode, domain name, and VLAN configurations in the switch startup configuration file and reboot the switch, the VTP and VLAN configurations are determined by these conditions:

- If both the VLAN database and the configuration file show the VTP mode as transparent and the VTP domain names match, the VLAN database is ignored. The VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the startup VTP mode is server mode, or the startup VTP mode or domain names do not match the VLAN database, VTP mode and VLAN configuration for the first 1005 VLANs are determined by VLAN database information, and VLANs greater than 1005 are configured from the switch configuration file.

The **vtp file** *filename* cannot be used to load a new database; it renames only the file in which the existing database is stored.

Follow these guidelines when configuring a VTP domain name:

- The switch is in the no-management-domain state until you configure a domain name. While in the no-management-domain state, the switch does not send any VTP advertisements even if changes occur to the local VLAN configuration. The switch leaves the no-management-domain state after it receives the first VTP summary packet on any port that is trunking or after you configure a domain name by using the **vtp domain** command. If the switch receives its domain from a summary packet, it resets its configuration revision number to 0. After the switch leaves the no-management-domain state, it can no be configured to re-enter it until you clear the NVRAM and reload the software.
- Domain names are case sensitive.
- After you configure a domain name, it cannot be removed. You can only reassign it to a different domain.

Follow these guidelines when setting VTP mode:

- The **no vtp mode** command returns the switch to VTP server mode.
- The **vtp mode server** command is the same as **no vtp mode** except that it does not return an error if the switch is not in client or transparent mode.

- If the receiving switch is in client mode, the client switch changes its configuration to duplicate the configuration of the server. If you have switches in client mode, be sure to make all VTP or VLAN configuration changes on a switch in server mode. If the receiving switch is in server mode or transparent mode, the switch configuration is not changed.
- Switches in transparent mode do not participate in VTP. If you make VTP or VLAN configuration changes on a switch in transparent mode, the changes are not propagated to other switches in the network.
- If you change the VTP or VLAN configuration on a switch that is in server mode, that change is propagated to all the switches in the same VTP domain.
- The **vtp mode transparent** command disables VTP from the domain but does not remove the domain from the switch.
- The VTP mode must be transparent for you to add extended-range VLANs or for VTP and VLAN information to be saved in the running configuration file.
- If extended-range VLANs are configured on the switch and you attempt to set the VTP mode to server or client, you receive an error message, and the configuration is not allowed.
- VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.

Follow these guidelines when setting a VTP password:

- Passwords are case sensitive. Passwords should match on all switches in the same domain.
- When you use the **no vtp password** form of the command, the switch returns to the no-password state.

Follow these guidelines when setting VTP pruning:

- VTP pruning removes information about each pruning-eligible VLAN from VTP updates if there are no stations belonging to that VLAN.
- If you enable pruning on the VTP server, it is enabled for the entire management domain for VLAN IDs 1 to 1005.
- Only VLANs in the pruning-eligible list can be pruned.
- Pruning is supported with VTP version 1 and version 2.

Follow these guidelines when setting the VTP version:

- Toggling the version 2 (v2) mode state modifies parameters of certain default VLANs.
- Each VTP switch automatically detects the capabilities of all the other VTP devices. To use version 2, all VTP switches in the network must support version 2; otherwise, you must configure them to operate in VTP version 1 mode.
- If all switches in a domain are VTP version 2-capable, you need only to configure version 2 on one switch; the version number is then propagated to the other version-2 capable switches in the VTP domain.
- If you are using VTP in a Token Ring environment, VTP version 2 must be enabled.
- If you are configuring a Token Ring bridge relay function (TrBRF) or Token Ring concentrator relay function (TrCRF) VLAN media type, you must use version 2.
- If you are configuring a Token Ring or Token Ring-NET VLAN media type, you must use version 1.

You cannot save password, pruning, and version configurations in the switch configuration file.

Examples

This example shows how to rename the filename for VTP configuration storage to *vtpfilename*:

```
Switch(config)# vtp file vtpfilename
```

This example shows how to clear the device storage filename:

```
Switch(config)# no vtp file vtpconfig
Clearing device storage filename.
```

This example shows how to specify the name of the interface providing the VTP updater ID for this device:

```
Switch(config)# vtp interface gigabitethernet
```

This example shows how to set the administrative domain for the switch:

```
Switch(config)# vtp domain OurDomainName
```

This example shows how to place the switch in VTP transparent mode:

```
Switch(config)# vtp mode transparent
```

This example shows how to configure the VTP domain password:

```
Switch(config)# vtp password ThisIsOurDomain'sPassword
```

This example shows how to enable pruning in the VLAN database:

```
Switch(config)# vtp pruning
Pruning switched ON
```

This example shows how to enable version 2 mode in the VLAN database:

```
Switch(config)# vtp version 2
```

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

Related Commands

Command	Description
show vtp status	Displays the VTP statistics for the switch and general information about the VTP management domain status.
vtp (VLAN configuration)	Configures VTP domain-name, password, pruning, version, and mode.

vtp (VLAN configuration)

Use the **vtp** VLAN configuration command to configure VLAN Trunking Protocol (VTP) characteristics. You access VLAN configuration mode by entering the **vlan database** privileged EXEC command. Use the **no** form of this command to return to the default settings, disable the characteristic, or remove the password.

```
vtp {domain domain-name | password password | pruning | v2-mode | {server | client | transparent}}
```

```
no vtp {client | password | pruning | transparent | v2-mode}
```


Note

VTP configuration in VLAN configuration mode is saved in the VLAN database when applied.

Syntax Description

domain <i>domain-name</i>	Set the VTP domain name by entering an ASCII string from 1 to 32 characters that identifies the VTP administrative domain for the switch. The domain name is case sensitive.
password <i>password</i>	Set the administrative domain password for the generation of the 16-byte secret value used in MD5 digest calculation to be sent in VTP advertisements and to validate received VTP advertisements. The password can be an ASCII string from 1 to 32 characters. The password is case sensitive.
pruning	Enable pruning in the VTP administrative domain. VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if there are no stations belonging to that VLAN.
v2-mode	Enable VLAN Trunking Protocol (VTP) version 2 in the administrative domains.
client	Place the switch in VTP client mode. A switch in VTP client mode is enabled for VTP, can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on it. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database.
server	Place the switch in VTP server mode. A switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The switch can recover all the VLAN information in the current VTP database from nonvolatile storage after reboot.
transparent	Place the switch in VTP transparent mode. A switch in VTP transparent mode is disabled for VTP, does not send advertisements or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The switch receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received.

Defaults

The default mode is server mode.

No domain name is defined.

No password is configured.

Pruning is disabled.

VTP version 2 (v2 mode) is disabled.

Command Modes

VLAN configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

If the VTP mode is transparent, the mode and domain name are saved in the switch running configuration file, and you can save the configuration in the switch startup configuration file by using the **copy running-config startup-config** privileged EXEC command.

Follow these guidelines when setting the VTP mode:

- The **no vtp client** and **no vtp transparent** forms of the command return the switch to VTP server mode.
- The **vtp server** command is the same as **no vtp client** or **no vtp transparent** except that it does not return an error if the switch is not in client or transparent mode.
- If the receiving switch is in client mode, the client switch changes its configuration to duplicate the configuration of the server. If you have switches in client mode, make sure to make all VTP or VLAN configuration changes on a switch in server mode. If the receiving switch is in server mode or transparent mode, the switch configuration is not changed.
- Switches in transparent mode do not participate in VTP. If you make VTP or VLAN configuration changes on a switch in transparent mode, the changes are not propagated to other switches in the network.
- If you make a change to the VTP or VLAN configuration on a switch in server mode, that change is propagated to all the switches in the same VTP domain.
- The **vtp transparent** command disables VTP from the domain but does not remove the domain from the switch.
- The VTP mode must be transparent for you to add extended-range VLANs or for the VTP and the VLAN configurations to be saved in the running configuration file.
- If extended-range VLANs are configured on the switch and you attempt to set the VTP mode to server or client, you receive an error message and the configuration is not allowed.
- VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.

Follow these guidelines when configuring a VTP domain name:

- The switch is in the no-management-domain state until you configure a domain name. While in the no-management-domain state, the switch does not send any VTP advertisements even if changes occur to the local VLAN configuration. The switch leaves the no-management-domain state after receiving the first VTP summary packet on any port that is currently trunking or after configuring a domain name with the **vtp domain** command. If the switch receives its domain from a summary

packet, it resets its configuration revision number to zero. After the switch leaves the no-management-domain state, it can never be configured to reenter it until you clear the NVRAM and reload the software.

- Domain names are case sensitive.
- After you configure a domain name, it cannot be removed. You can reassign it only to a different domain.

Follow these guidelines when configuring a VTP password:

- Passwords are case sensitive. Passwords should match on all switches in the same domain.
- When the **no vtp password** form of the command is used, the switch returns to the no-password state.

Follow these guidelines when enabling VTP pruning:

- If you enable pruning on the VTP server, it is enabled for the entire management domain.
- Only VLANs included in the pruning-eligible list can be pruned.
- Pruning is supported with VTP version 1 and version 2.

Follow these guidelines when enabling VTP version 2 (v2-mode):

- Toggling the version (v2-mode) state modifies certain parameters of certain default VLANs.
- Each VTP switch automatically detects the capabilities of all the other VTP devices. To use VTP version 2, all VTP switches in the network must support version 2; otherwise, you must configure them to operate in VTP version 1 (**no vtp v2-mode**).
- If all switches in a domain are VTP version 2-capable, you need only to enable VTP version 2 on one switch; the version number is then propagated to the other version-2 capable switches in the VTP domain.
- If you are using VTP in a Token Ring environment or configuring a Token Ring bridge relay function (TrBRF) or Token Ring concentrator relay function (TrCRF) VLAN media type, VTP version 2 (**v2-mode**) must be enabled.
- If you are configuring a Token Ring or Token Ring-NET VLAN media type, you must use VTP version 1.

Examples

This example shows how to place the switch in VTP transparent mode:

```
Switch(vlan)# vtp transparent  
Setting device to VTP TRANSPARENT mode.
```

This example shows how to set the administrative domain for the switch:

```
Switch(vlan)# vtp domain OurDomainName  
Changing VTP domain name from cisco to OurDomainName
```

This example shows how to configure the VTP domain password:

```
Switch(vlan)# vtp password private  
Setting device VLAN database password to private.
```

This example shows how to enable pruning in the proposed new VLAN database:

```
Switch(vlan)# vtp pruning  
Pruning switched ON
```

This example shows how to enable v2 mode in the proposed new VLAN database:

```
Switch(vlan)# vtp v2-mode  
V2 mode enabled.
```

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

Related Commands	Command	Description
	show vtp status	Displays the VTP statistics for the switch and general information about the VTP management domain status.
	switchport trunk pruning	Configures the VLAN pruning-eligible list for ports in trunking mode.
	vtp (global configuration)	Configures the VTP filename, interface, domain name, and mode.

xconnect

Use the **xconnect** interface configuration command at customer-edge (CE) or service provider-edge (PE) ingress and egress Ethernet ports or VLAN interfaces with a destination and virtual-connection (VC) ID to route a Layer 2 packets over a specified point-to-point VC by using Ethernet over multiprotocol label switching (EoMPLS). You can also bind the VC to a pseudowire. Use the **no** form of this command on both edge devices to delete the VC.

xconnect *destination vc-id* {**encapsulation mpls** [**pw-class** *pw-class-name*]}

no xconnect



Note

This command will replace the **mpls l2transport route** interface configuration command.

Syntax Description

<i>destination</i>	The destination label distribution protocol (LDP) IP address of the remote provider edge device. The IP address cannot be an IP address on the route on which the command is entered.
<i>vc-id</i>	Assign a virtual connection identifier (VC ID) for the virtual connection between the two peer provider edge devices. The range is 1 to 4294967295.
encapsulation mpls	Specify the MPLS data encapsulation method.
pw-class <i>pw-class-name</i>	(Optional) Specify the pseudowire class for advanced configuration.

Defaults

There are no point-to-point connections configured.

When configured, the attachment circuit is not bound to the pseudowire.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)AX	This command was introduced.
12.2(25)EY	The encapsulation mpls keywords were added.
12.2(46)SE	The pw-class <i>pw-class-name</i> keywords were added.

Usage Guidelines

An MPLS VC runs across an MPLS cloud to connect Ethernet interfaces on two provider edge devices at each edge of the service provider network. You must enter the command at the PE device at each edge of the service provider network to establish a bidirectional virtual connection, which consists of two unidirectional label-switched paths (LSPs). A VC is not established if not properly defined from both ends.

For the *destination* parameter, specify the LDP IP address of the other PE device; do not specify the IP address of the device on which you are entering the command.

The *vc-id* must be unique for each pair of provider edge devices. Therefore, in large networks, you should keep track of the VC ID assignments to ensure that a VC ID is not assigned more than once.

The **pw-class** keyword with the *pw-class-name* value binds the xconnect configuration of an attachment circuit to a specific pseudowire class. In this way, the pseudowire class configuration serves as a template that contains settings used by all attachment circuits bound to it with the xconnect command.

To configure the pseudowire class, use the **pseudowire-class** global configuration command to enter pseudo-wire class configuration mode. See the IOS documentation for this command.

http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_m4.html#wp1015442

The Catalyst 3750 Metro switch supports only the **encapsulation mpls** and **preferred-path** options in pseudo-wire configuration mode.

Examples

This example shows how to establish an Ethernet over MPLS (EoMPLS) tunnel between the PE1 VLAN 3 interface and the PE2 VLAN 4 interface. PE1 has IP address 10.0.0.1/32 that PE2 discovers through routing and PE2 has IP address 20.0.0.1/32 that PE1 discovers through routing.

At the PE1 interface:

```
Switch(config)# interface vlan 3
Switch(config-if)# xconnect 20.0.0.1 123 encapsulation mpls
```

At the PE2 interface:

```
Switch(config)# interface vlan 4
Switch(config-if)# xconnect 10.0.0.1 123 encapsulation mpls
```

This example shows how to configure a pseudowire class named *vc-class* and then configure xconnect service for an interface by binding the interface to the pseudowire named *123* with a remote peer *10.0.3.201*. The configuration uses the settings in the pseudowire class.

```
Switch (config)# pseudowire-class vc-class
Switch (config-pw-class)# encapsulation mpls
Switch (config-pw-class)# preferred-path interface tunnel 100
Switch (config-pw-class)# exit
Switch(config)# interface Gigabit Ethernet 1/0/1
Switch(config-if)# xconnect 10.0.3.201 123 pw-class vc-class
```

You can verify your setting by entering the **show mpls2 transport vc** privileged EXEC command.

Related Commands

Command	Description
show mpls l2transport vc	Displays information about the EoMPLS VCs that have been enabled to route Layer 2 packets on a device.



APPENDIX **A**

Catalyst 3750 Metro Switch Boot Loader Commands

This appendix describes the boot loader commands on the Catalyst 3750 Metro 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 switch default 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. Unplug the switch power cord, and press the switch **Mode** button while reconnecting the power cord. You can release the **Mode** button a second or two after the LED above port 1X goes off. You should then see the boot loader *Switch:* prompt. The boot loader performs low-level CPU initialization, performs POST, and loads a default operating system image into memory.

boot

Use the **boot** boot loader command to load and boot an executable image and to enter the command-line interface.

boot [-post | -n | -p | *flag*] *filesystem:/file-url* ...

Syntax Description

-post	(Optional) Run the loaded image with an extended or comprehensive power-on self-test (POST). Using this keyword causes POST to take longer to complete.
-n	(Optional) Pause for the Cisco IOS debugger immediately after launching.
-p	(Optional) Pause for the JTAG debugger right after loading the image.
<i>filesystem:</i>	Alias for a flash file system. Use flash: 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
12.1(14)AX	This command was introduced.

Usage Guidelines

When you enter the **boot** command without any arguments, the switch attempts to automatically boot the system by using the information in the BOOT environment variable, if any. If you supply an image name for the *file-url* variable, the **boot** command attempts to boot the specified image.

When you set boot loader **boot** command options, they are executed immediately and apply only to the current boot loader session. These settings are not saved for the next boot operation.

Filenames and directory names are case sensitive.

Examples

This example shows how to boot the switch using the *new-image.bin* image:

```
switch: boot flash:/new-images/new-image.bin
```

After entering this command, you are prompted to start the setup program.

Related Commands	Command	Description
	set	Sets the BOOT environment variable to boot a specific image when the BOOT keyword is appended to the command.

cat

Use the **cat** boot loader command to display the contents of one or more files.

cat *filesystem:/file-url* ...

Syntax Description

<i>filesystem:</i>	Alias for a flash file system. Use flash: 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
12.1(14)AX	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 is sequentially displayed.

Examples

This example shows how to display the contents of two files, *info* and *env_vars*:

```
switch: cat flash:/new-images/info flash:env_vars
```

Related Commands

Command	Description
more	Displays the contents of one or more files.
type	Displays the contents of one or more files.

copy

Use the **copy** boot loader command to copy a file from a source to a destination.

copy [-b *block-size*] *filesystem:/source-file-url filesystem:/destination-file-url*

Syntax Description	-b <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 flash: 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
	12.1(14)AX	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Filenames are limited to 45 characters; the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

If you are copying a file to a new directory, the directory must already exist.

Examples

This example show how to copy a file at the root:

```
switch: copy flash:test1.text flash:test4.text
.
```

File "flash:test1.text" successfully copied to "flash:test4.text"

You can verify that the file was copied by entering the **dir** *filesystem:* boot loader command.

Related Commands	Command	Description
	delete	Deletes one or more files from the specified file system.

delete

Use the **delete** boot loader command to delete one or more files from the specified file system.

delete *filesystem:/file-url ...*

Syntax Description	<i>filesystem:</i>	Alias for a flash file system. Use flash: 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
	12.1(14)AX	This command was introduced.

Usage Guidelines	Filenames and directory names are case sensitive.
	The switch prompts you for confirmation before deleting each file.

Examples	This example shows how to delete two files:
	<pre>switch: delete flash:test2.text flash:test5.text Are you sure you want to delete "flash:test2.text" (y/n)? y File "flash:test2.text" deleted Are you sure you want to delete "flash:test5.text" (y/n)? y File "flash:test2.text" deleted</pre>

You can verify that the files were deleted by entering the **dir flash:** boot loader command.

Related Commands	Command	Description
	copy	Copies a file from a source to a destination.

dir

Use the **dir** boot loader command to display a list of files and directories on the specified file system.

dir *filesystem:/file-url* ...

Syntax Description	<i>filesystem:</i>	Alias for a flash file system. Use flash: 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
	12.1(14)AX	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  c3750me-i5-mz.121-14.35.AX
```

15998976 bytes total (6397440 bytes free)

Table A-1 describes the fields in the display.

Table A-1 *dir* Field Descriptions

Field	Description
3	Index number of the file.
-rwx	File permission, which can be any or all of the following: - d—directory - r—readable - w—writable - x—executable

Table A-1 *dir Field Descriptions (continued)*

Field	Description
1839	Size of the file.
<date>	Last modification date.
env_vars	Filename.

Related Commands

Command	Description
mkdir	Creates one or more directories.
rmdir	Removes one or more directories.

flash_init

Use the **flash_init** boot loader command to initialize the flash file system.

flash_init

Syntax Description	This command has no arguments or keywords.

Defaults	The flash file system is automatically initialized during normal system operation.

Command Modes	Boot loader

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	During the normal boot process, the flash file system is automatically initialized.
	Use this command to manually initialize the flash file system. For example, you use this command during the recovery procedure for a lost or forgotten password.

format

Use the **format** boot loader command to format the specified file system and destroy all data in that file system.

format *filesystem:*

Syntax Description	<i>filesystem:</i> Alias for a flash file system. Use flash: for the system board flash device.

Command Modes	Boot loader

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines



Caution

Use this command with care; it destroys all data on the file system and renders your system unusable.

fsck

Use the **fsck** boot loader command to check the file system for consistency.

fsck [-f | -test] *filesystem:*

Syntax Description	-f	(Optional) Initialize the file system code and perform a fast file consistency check. Cyclic redundancy checks (CRCs) in the flashfs sectors are not checked.
	-test	(Optional) Initialize the file system code and perform extra POST on flash memory. An extensive, nondestructive memory test is performed on every byte that makes up the file system.
	<i>filesystem:</i>	Alias for a flash file system. Use flash: for the system board flash device.

Defaults	No file system check is performed.

Command Modes	Boot loader

Command History	Release	Modification
	12.1(14)AX	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: <pre>switch: fsck -test flash:</pre>

help

Use the **help** boot loader command to display the available commands.

help

Syntax Description This command has no arguments or keywords.

Command Modes Boot loader

Command History	Release	Modification
	12.1(14)AX	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
	12.1(14)AX	This command was introduced.

Examples This example shows how to display memory heap utilization information:

```
switch: memory
Text: 0x07d807c0 - 0x07da73a8 (0x00026be8 bytes)
Rotext: 0x07da73a8 - 0x07da73a8 (0x00000000 bytes)
Data: 0x07da73a8 - 0x07dadf18 (0x00006b70 bytes)
Bss: 0x07daf4c0 - 0x07dd157c (0x000220bc bytes)
Stack: 0x07dd157c - 0x07de157c (0x00010000 bytes)
Heap: 0x07de1580 - 0x07ffdfc0 (0x0021ca40 bytes)
```

Bottom heap utilization is 53 percent.

Top heap utilization is 0 percent.

Total heap utilization is 53 percent.

Total bytes: 0x21ca40 (2214464)

Bytes used: 0x120960 (1182048)

Bytes available: 0xfc0e0 (1032416)

Alternate heap utilization is 3 percent.

Total alternate heap bytes: 0x7d7d7c0 (131585984)

Alternate heap bytes used: 0x400004 (4194308)

Alternate heap bytes available: 0x797d7bc (127391676)

Table A-2 describes the fields in the display.

Table A-2 *memory Field Descriptions*

Field	Description
Text	Beginning and ending address of the text storage area.
Rotext	Beginning and ending address of the read-only text storage area. This part of the data segment is grouped with the Text entry.
Data	Beginning and ending address of the data segment storage area.
Bss	Beginning and ending address of the block started by symbol (Bss) storage area. It is initialized to zero.

Table A-2 *memory Field Descriptions (continued)*

Field	Description
Stack	Beginning and ending address of the area in memory allocated to the software to store automatic variables, return addresses, and so forth.
Heap	Beginning and ending address of the area in memory that memory is dynamically allocated to and freed from.

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 flash: 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
	12.1(14)AX	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 <i>Saved_Configs</i> :

```
switch: mkdir flash:Saved_Configs
Directory "flash:Saved_Configs" created
```

This example shows how to make two directories:

```
switch: mkdir flash:Saved_Configs1 flash:Test
Directory "flash:Saved_Configs1" created
Directory "flash:Test" created
```

You can verify that the directory was created by entering the **dir** *filesystem:* boot loader command.

Related Commands	Command	Description
	dir	Displays a list of files and directories on the specified file system.
	rmdir	Removes one or more directories from the specified file system.

more

Use the **more** boot loader command to display the contents of one or more files.

more *filesystem:/file-url* ...

Syntax Description	<i>filesystem:</i>	Alias for a flash file system. Use flash: 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
	12.1(14)AX	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 is sequentially displayed.

Examples	This example shows how to display the contents of two files, <i>info</i> and <i>env_vars</i> :
	switch: more flash:/new-images/info flash:env_vars

Related Commands	Command	Description
	cat	Displays the contents of one or more files.
	type	Displays the contents of one or more files.

rename

Use the **rename** boot loader command to rename a file.

rename *filesystem:/source-file-url filesystem:/destination-file-url*

Syntax Description	<i>filesystem:</i>	Alias for a flash file system. Use flash: 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
	12.1(14)AX	This command was introduced.

Usage Guidelines	Filenames and directory names are case sensitive.
	Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.
	Filenames are limited to 45 characters; the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Examples	This example shows a file named <i>config.text</i> being renamed to <i>config1.text</i> :
	switch: rename flash:config.text flash:config1.text
	You can verify that the file was renamed by entering the dir filesystem: boot loader command.

Related Commands	Command	Description
	copy	Copies a file from a source to a destination.

reset

Use the **reset** boot loader command to perform a hard reset on the system. A hard reset is similar to power-cycling the switch, clearing the processor, registers, and memory.

reset

Syntax Description	This command has no arguments or keywords.

Command Modes	Boot loader

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Examples	This example shows how to reset the system:

```
switch: reset
Are you sure you want to reset the system (y/n)? y
System resetting...
```

Related Commands	Command	Description
	boot	Loads and boots an executable image and enters the command-line interface.

rmdir

Use the **rmdir** boot loader command to remove one or more empty directories from the specified file system.

rmdir *filesystem:/directory-url* ...

Syntax Description

<i>filesystem:</i>	Alias for a flash file system. Use flash: 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
12.1(14)AX	This command was introduced.

Usage Guidelines

Directory names are case sensitive and limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Before removing a directory, you must first delete all the files in the directory.

The switch prompts you for confirmation before deleting each directory.

Examples

This example shows how to remove a directory:

```
switch: rmdir flash:Test
```

You can verify that the directory was deleted by entering the **dir** *filesystem:* boot loader command.

Related Commands

Command	Description
dir	Displays a list of files and directories on the specified file system.
mkdir	Creates one or more new directories on the specified file system.

set

Use the **set** boot loader command to set or display environment variables, which can be used to control the boot loader or any other software running on the switch.

set *variable value*



Note

Under normal circumstances, it is not necessary to alter the setting of the environment variables.

Syntax Description

<i>variable value</i>	Use one of these keywords for <i>variable</i> and <i>value</i>: MANUAL_BOO—Determines whether the switch automatically or manually boots. Valid values are 1, yes, 0, and no. If it is set to no or 0, the boot loader attempts to automatically boot the system. If it is set to anything else, you must manually boot the switch from the boot loader mode. BOOT filesystem:/file-url—A semicolon-separated list of executable files to try to load and execute when automatically booting. If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash: file system. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash file system. ENABLE_BREAK—Determines whether the automatic boot process can be interrupted by using the Break key on the console. Valid values are 1, yes, on, 0, no, and off. If it is set to 1, yes, or on, you can interrupt the automatic boot process by pressing the Break key on the console after the flash file system has initialized. HELPER filesystem:/file-url—A semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader. PS1 prompt—A string that is used as the command-line prompt in boot loader mode. CONFIG_FILE flash:/file-url—The filename that the software uses to read and write a nonvolatile copy of the system configuration.

BAUD rate—The rate in bits per second (bps) used for the console. The 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.

The most commonly used values are 300, 1200, 2400, 9600, 19200, 57600, and 115200.

HELPER_CONFIG_FILE *filesystem:/file-url*—The name of the configuration file to be used by the helper image. If this is not set, the file specified by the CONFIG_FILE environment variable is used by all versions of software that are loaded, including the helper image. This variable is used only for internal development and testing.

Defaults

The environment variables have these default values:

MANUAL_BOOT: No (0)

BOOT: Null string

ENABLE_BREAK: No (Off or 0) (the automatic boot process cannot be interrupted by pressing the Break key on the console).

HELPER: No default value (helper files are not automatically loaded).

PS1: switch:

CONFIG_FILE: config.text

BAUD: 9600 bps

HELPER_CONFIG_FILE: No default value (no helper configuration file is specified).



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
12.1(14)AX	This command was introduced.

Usage Guidelines

Environment variables are case sensitive and must be entered as documented.

Environment variables that have values are stored in flash memory outside of the flash file system.

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
unset	Resets one or more environment variables to its previous setting.

type

Use the **type** boot loader command to display the contents of one or more files.

type *filesystem:/file-url* ...

Syntax Description	<i>filesystem:</i>	Alias for a flash file system. Use flash: 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
	12.1(14)AX	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 is sequentially displayed.

Examples	This example shows how to display the contents of two files: switch: type flash:/new-images/info flash:env_vars

Related Commands	Command	Description
	cat	Displays the contents of one or more files.
	more	Displays the contents of one or more files.

unset

Use the **unset** boot loader command to reset one or more environment variables.

unset *variable* ...

**Note**

Under normal circumstances, it is not necessary to alter the setting of the environment variables.

Syntax Description

<i>variable</i>	Use one of these keywords for <i>variable</i> : MANUAL_BOOT —Determines 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 —Determines 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 the software 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 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 helper image. If this is not set, the file specified by the CONFIG_FILE environment variable is used by all versions of the software 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
12.1(14)AX	This command was introduced.

Usage Guidelines

The MANUAL_BOOT environment variable can also be reset by using the **no boot manual** global configuration command.

The BOOT environment variable can also be reset by using the **no boot system** global configuration command.

The ENABLE_BREAK environment variable can also be reset by using the **no boot enable-break** global configuration command.

The HELPER environment variable can also be reset by using the **no boot helper** global configuration command.

The CONFIG_FILE environment variable can also be reset by using the **no boot config-file** global configuration command.

The HELPER_CONFIG_FILE environment variable can also be reset by using the **no boot helper-config-file** global configuration command.

Examples

This example shows how to reset the prompt string to its previous setting:

```
switch: unset PS1
switch:
```

Related Commands

Command	Description
set	Sets or displays environment variables.

version

Use the **version** boot loader command to display the boot loader version.

version

Syntax Description

This command has no arguments or keywords.

Command Modes

Boot loader

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Examples

This example shows how to display the boot loader version:

```
switch: version
Boot Loader (HULC-HBOOT-M), Version 12.1 [mbutts-congo_bl 116]
compiled Sat 19-Apr-03 17:02 by mbutts
```




APPENDIX **B**

Catalyst 3750 Metro Switch Debug Commands

This appendix describes the **debug** privileged EXEC commands that have been created or changed for use with the Catalyst 3750 Metro 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 auto qos

Use the **debug auto qos** privileged EXEC command to enable debugging of the automatic quality of service (auto-QoS) feature. Use the **no** form of this command to disable debugging.

debug auto qos

no debug auto qos

Syntax Description This command has no arguments or keywords.

Defaults Auto-QoS debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.
	12.2(25)EY	The debug auto qos command replaced the debug autoqos command.

Usage Guidelines To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging *before* you enable auto-QoS. You enable debugging by entering the **debug autoqos** privileged EXEC command.

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

Examples This example shows how to display the QoS configuration that is automatically generated when auto-QoS is enabled:

```
Switch# debug autoqos
AutoQoS debugging is on
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# auto qos voip cisco-phone

21:29:41: mls qos map cos-dscp 0 8 16 26 32 46 48 56
21:29:41: mls qos
21:29:42: no mls qos srr-queue input cos-map
21:29:42: no mls qos srr-queue output cos-map
21:29:42: mls qos srr-queue input cos-map queue 1 threshold 3 0
21:29:42: mls qos srr-queue input cos-map queue 1 threshold 2 1
21:29:42: mls qos srr-queue input cos-map queue 2 threshold 1 2
21:29:42: mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7
21:29:43: mls qos srr-queue input cos-map queue 2 threshold 3 3 5
21:29:43: mls qos srr-queue output cos-map queue 1 threshold 3 5
21:29:43: mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7
21:29:44: mls qos srr-queue output cos-map queue 3 threshold 3 2 4
```

```

21:29:44: mls qos srr-queue output cos-map queue 4 threshold 2 1
21:29:44: mls qos srr-queue output cos-map queue 4 threshold 3 0
21:29:44: no mls qos srr-queue input dscp-map
21:29:44: no mls qos srr-queue output dscp-map
21:29:44: mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15
21:29:45: mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7
21:29:45: mls qos srr-queue input dscp-map queue 1 threshold 3 32
21:29:45: mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
21:29:45: mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48
21:29:46: mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56
21:29:46: mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63
21:29:46: mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
21:29:47: mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47
21:29:47: mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47
21:29:47: mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
21:29:47: mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
21:29:48: mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
21:29:48: mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23
21:29:48: mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39
21:29:49: mls qos srr-queue output dscp-map queue 4 threshold 1 8
21:29:49: mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15
21:29:49: mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7
21:29:49: no mls qos srr-queue input priority-queue 1
21:29:49: no mls qos srr-queue input priority-queue 2
21:29:50: mls qos srr-queue input bandwidth 90 10
21:29:50: no mls qos srr-queue input buffers
21:29:50: mls qos queue-set output 1 buffers 10 10 26 54
21:29:50: interface GigabitEthernet1/0/1
21:29:50: mls qos trust device cisco-phone
21:29:50: mls qos trust cos
21:29:50: no queue-set 1
21:29:50: srr-queue bandwidth shape 10 0 0 0
21:29:50: srr-queue bandwidth share 10 10 60 20

```

Related Commands

Command	Description
auto qos voip	Configures auto-QoS for voice over IP (VoIP) within a QoS domain.
show auto qos	Displays the initial configuration that is generated by the automatic auto-QoS feature
show debugging	Displays information about the types of debugging that are enabled.

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

all	Display all backup interface debug messages.
errors	Display backup interface error or exception debug messages.
events	Display backup interface event debug messages.
vlan-load-balancing	Display backup interface VLAN load balancing.

Command Default

Backup interface debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)EY	This command was introduced.
12.2(37)SE	Added vlan-load-balancing keyword.

Usage Guidelines

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

Related Commands

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

debug cluster

Use the **debug cluster** privileged EXEC command to enable debugging of cluster-specific events. Use the **no** form of this command to disable debugging.

```
debug cluster { discovery | events | extended | hsrp | http | ip [packet] | members | nat | neighbors
               | platform | snmp | vqpxy }
```

```
no debug cluster { discovery | events | extended | hsrp | http | ip [packet] | members | nat |
                 neighbors | platform | snmp | vqpxy }
```

Syntax Description		
discovery		Display cluster discovery debug messages.
events		Display cluster event debug messages.
extended		Display extended discovery debug messages.
hsrp		Display the Hot Standby Router Protocol (HSRP) debug messages.
http		Display HTTP debug messages.
ip [packet]		Display IP or transport packet debug messages.
members		Display cluster member debug messages.
nat		Display Network Address Translation (NAT) debug messages.
neighbors		Display cluster neighbor debug messages.
platform		Display platform-specific cluster debug messages.
snmp		Display Simple Network Management Protocol (SNMP) debug messages.
vqpxy		Display VLAN Query Protocol (VQP) proxy debug messages.

Defaults Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines This command is available only on the cluster command switch.
The **undebg cluster** command is the same as the **no debug cluster** command.

Related Commands	Command	Description
	show debugging	Displays information about the types of debugging that are enabled.
	show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.

Command	Description
show cluster candidates	Displays a list of candidate switches when entered on the command switch.
show cluster members	Displays information about cluster members when executed on the command switch.

debug dot1x

Use the **debug dot1x** privileged EXEC command to enable debugging of the 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	all	Display all 802.1x debug messages.
	errors	Display 802.1x error debug messages.
	events	Display 802.1x event debug messages.
	packets	Display 802.1x packet debug messages.
	registry	Display 802.1x registry invocation debug messages.
	state-machine	Display state-machine related-events debug messages.

Defaults	Debugging is disabled.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	The undebg dot1x command is the same as the no debug dot1x command.

Related Commands	Command	Description
	show debugging	Displays information about the types of debugging that are enabled.
	show dot1x	Displays 802.1x statistics, administrative status, and operational status for the switch or for the specified port.

debug dtp

Use the **debug dtp** privileged EXEC command to enable debugging of the Dynamic Trunking Protocol (DTP) activity. Use the **no** form of this command to disable debugging.

debug dtp {aggregation | all | decision | events | oserrs | packets | queue | states | timers}

no debug dtp {aggregation | all | decision | events | oserrs | packets | queue | states | timers}

Syntax Description

aggregation	Display DTP user-message aggregation debug messages.
all	Display all DTP debug messages.
decision	Display the DTP decision-table debug messages.
events	Display the DTP event debug messages.
oserrs	Display DTP operating system-related error debug messages.
packets	Display DTP packet-processing debug messages.
queue	Display DTP packet-queueing debug messages.
states	Display DTP state-transition debug messages.
timers	Display DTP timer-event debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

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

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show dtp	Displays DTP information for the switch or for a specified interface.

debug etherchannel

Use the **debug etherchannel** privileged EXEC command to enable debugging of the EtherChannel/PAgP shim. This shim is the software module that is the interface between the Port Aggregation Protocol (PAgP) software module and the port manager software module. Use the **no** form of this command to disable debugging.

debug etherchannel [**all** | **detail** | **error** | **event** | **idb**]

no debug etherchannel [**all** | **detail** | **error** | **event** | **idb**]

Syntax Description

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



Note

Though visible in the command-line help strings, the **linecard** keyword is not supported.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

If you do not specify a keyword, all debug messages are displayed.

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

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show etherchannel	Displays EtherChannel information for the channel.

debug 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		
all		Display all Ethernet customer-service debug messages.
api		Display debug messages about the interaction between the Ethernet infrastructure and its clients.
error		Display Ethernet customer-service error messages occurring in the Ethernet infrastructure subsystem.
evc		Display Ethernet virtual connection (EVC) debug messages
id <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.
instance		Display debug messages related to Ethernet customer-service instances.
id <i>id</i> <i>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.
interface <i>interface-id</i>		(Optional) When entered after the instance keyword, display service-instance debug messages for the interface. You must enter an interface ID.
interface [<i>interface-id</i>]		Display debugging for Ethernet services on all interfaces or the specified interface.
oam-mgr		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(25)SEG	This command was introduced.

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

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

debug interface

Use the **debug interface** privileged EXEC command to enable debugging of port-related activities. Use the **no** form of this command to disable debugging.

debug interface {*interface-id* | **null** *interface-number* | **port-channel** *port-channel-number* | **tunnel** *tunnel-interface* | **vlan** *vlan-id*}

no debug interface {*interface-id* | **null** *interface-number* | **port-channel** *port-channel-number* | **tunnel** *tunnel-interface* | **vlan** *vlan-id*}

Syntax Description		
<i>interface-id</i>		Display debug messages for the specified physical port, for example fastethernet1/0/3.
null <i>interface-number</i>		Display debug messages for null interfaces. The <i>interface-number</i> is always 0.
port-channel <i>port-channel-number</i>		Display debug messages for the specified EtherChannel port-channel. The <i>port-channel-number</i> range is 1 to 12.
tunnel <i>tunnel-interface</i>		Display debug messages for the specified Distance Vector Multicast Routing Protocol (DVMRP) tunnel. The <i>tunnel-interface</i> number range is 0 to 64.
vlan <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
	12.1(14)AX	This command was introduced.

Usage Guidelines If you do not specify a keyword, all debug messages are displayed.
The **undebug interface** command is the same as the **no debug interface** command.

Related Commands	Command	Description
	show debugging	Displays information about the types of debugging that are enabled.
	show etherchannel	Displays EtherChannel information for the channel.

debug ip 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.
agent	Display debug messages for DHCP snooping agents.
event	Display debug messages for DHCP snooping events.
packet	Display debug messages for DHCP snooping.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)EY	This command was introduced.

Usage Guidelines

The **undebg ip dhcp snooping** command is the same as the **no debug ip dhcp snooping** command.

Related Commands

Command	Description
show debugging	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
	12.1(14)AX	This command was introduced.

Usage Guidelines	The undebg ip igmp filter command is the same as the no debug ip igmp filter command.

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

debug ip igmp max-groups

Use the **debug ip igmp max-groups** privileged EXEC command to enable debugging of Internet Group Management Protocol (IGMP) maximum groups events. Use the **no** form of this command to disable debugging.

debug ip igmp max-groups

no debug ip igmp max-groups

Syntax Description	This command has no arguments or keywords.

Defaults	Debugging is disabled.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	The undebg ip igmp max-groups command is the same as the no debug ip igmp max-groups command.

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

debug ip igmp snooping

Use the **debug ip 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** | **router** | **timer**]

no debug ip igmp snooping [**group** | **management** | **router** | **timer**]

Syntax Description

group	(Optional) Display IGMP snooping group activity debug messages.
management	(Optional) Display IGMP snooping management activity debug messages.
router	(Optional) Display IGMP snooping router activity debug messages.
timer	(Optional) Display IGMP snooping timer event debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The **undebug ip igmp snooping** command is the same as the **no debug ip igmp snooping** command.

Related Commands

Command	Description
debug platform ip igmp snooping	Displays information about platform-dependent IGMP snooping activity.
show debugging	Displays information about the types of debugging that are enabled.

debug 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(25)EY	This command was introduced.

Usage Guidelines	The undebg ip verify source packet command is the same as the no debug ip verify source packet command.

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

debug lacp

Use the **debug lacp privileged EXEC** command to enable debugging of Link Aggregation Control Protocol (LACP) activity. Use the **no** form of this command to disable debugging.

debug lacp [**all** | **event** | **fsm** | **misc** | **packet**]

no debug lacp [**all** | **event** | **fsm** | **misc** | **packet**]

Syntax Description

all	(Optional) Display all LACP debug messages.
event	(Optional) Display LACP event debug messages.
fsm	(Optional) Display LACP finite state-machine debug messages.
misc	(Optional) Display miscellaneous LACP debug messages.
packet	(Optional) Display LACP packet debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

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

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show lacp	Displays LACP channel-group information.

debug 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
	12.1(14)AX	This command was introduced.

Usage Guidelines	The undebg mac-notification command is the same as the no debug mac-notification command.

Related Commands	Command	Description
	show debugging	Displays information about the types of debugging that are enabled.
	show mac address-table notification	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
	12.1(14)AX	This command was introduced.

Usage Guidelines	The undebg matm command is the same as the no debug matm command.

Related Commands	Command	Description
	debug platform matm	Displays information about platform-dependent MAC address management.
	show debugging	Displays information about the types of debugging that are enabled.

debug matm move update

Use the **debug matm move update** privileged EXEC command to enable debugging of MAC address-table move update message processing.

debug matm move update

no debug matm move update

Syntax Description	This command has no arguments or keywords.

Defaults	Debugging is disabled.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.2(25)SED	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
	mac address-table move update	Configures MAC address-table move update feature on the switch.
	show debugging	Displays information about the types of debugging that are enabled.
	show mac address-table move update	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

all	Display all SPAN debug messages.
errors	Display detailed SPAN error debug messages.
idb-update	Display SPAN interface description block (IDB) update-trace debug messages.
info	Display SPAN informational-tracing debug messages.
list	Display SPAN port and VLAN-list tracing debug messages.
notifications	Display SPAN notification debug messages.
platform	Display SPAN platform-tracing debug messages.
requests	Display SPAN request debug messages.
snmp	Display SPAN and Simple Network Management Protocol (SNMP) tracing debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The **undebg monitor** command is the same as the **no debug monitor** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show monitor	Displays information about all SPAN and remote SPAN (RSPAN) sessions on the switch.

debug mpls atom

Use the **debug mpls atom** privileged EXEC command to enable debugging of the Any Transport over multiprotocol label switching (AToM) layer. Use the **no** form of this command to disable debugging.

debug mpls atom

no debug mpls atom

**Note**

The Catalyst 3750 Metro switch supports Ethernet over MPLS (EoMPLS), a subset of AToM.

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Related Commands

Command	Description
debug mpls l2transport vlan	Enables debugging of EoMPLS Layer 2 VLANs.
show debugging	Displays information about the types of debugging that are enabled.

debug mpls l2transport vlan

Use the **debug mpls l2transport vlan** privileged EXEC command to enable debugging of the Ethernet over multiprotocol label switching (EoMPLS) Layer 2 VLANs. Use the **no** form of this command to disable debugging.

debug mpls l2transport vlan {control | distributed | switching}

no debug mpls l2transport vlan {control | distributed | switching}

Syntax Description

control	Display EoMPLS traffic control plane debug messages.
distributed	Display EoMPLS traffic distributed switching control debug messages.
switching	Display EoMPLS traffic packet switching debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Related Commands

Command	Description
debug mpls atom	Enables debugging of the Any Transport over multiprotocol label switching (AToM) layer.
show debugging	Displays information about the types of debugging that are enabled.
show mpls l2transport vc	Displays information about the Ethernet over MPLS (EoMPLS) virtual circuits (VCs).

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	all	Display all MVR activity debug messages.
	events	Display MVR event-handling debug messages.
	igmpsn	Display MVR Internet Group Management Protocol (IGMP) snooping-activity debug messages.
	management	Display MVR management-activity debug messages.
	ports	Display MVR port debug messages.

Defaults	Debugging is disabled.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	The undebg mvrdbg command is the same as the no debug mvrdbg command.

Related Commands	Command	Description
	show debugging	Displays information about the types of debugging that are enabled.
	show mvr	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
	12.1(14)AX	This command was introduced.

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

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

debug pagp

Use the **debug pagp** privileged EXEC command to enable debugging of Port Aggregation Protocol (PAgP) activity. Use the **no** form of this command to disable debugging.

debug pagp [**all** | **event** | **fsm** | **misc** | **packet**]

no debug pagp [**all** | **event** | **fsm** | **misc** | **packet**]

Syntax Description

all	(Optional) Display all PAgP debug messages.
event	(Optional) Display PAgP event debug messages.
fsm	(Optional) Display PAgP finite state-machine debug messages.
misc	(Optional) Display miscellaneous PAgP debug messages.
packet	(Optional) Display PAgP packet debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The **undebg pagp** command is the same as the **no debug pagp** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show pagp	Displays PAgP channel-group information.

debug platform acl

Use the **debug platform acl** privileged EXEC command to enable debugging of the access control list (ACL) manager. Use the **no** form of this command to disable debugging.

debug platform acl {all | exit | label | main | racl | vACL | vmap | warn}

no debug platform acl {all | exit | label | main | racl | vACL | vmap | warn}

Syntax Description

all	Display all ACL manager debug messages.
exit	Display ACL exit-related debug messages.
label	Display ACL label-related debug messages.
main	Display the main or important ACL debug messages.
racl	Display router ACL related debug messages.
vACL	Display VLAN ACL-related debug messages.
vmap	Display ACL VLAN-map-related debug messages.
warn	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
12.1(14)AX	This command was introduced.

Usage Guidelines

The **undebug platform acl** command is the same as the **no debug platform acl** command.

Related Commands

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

debug platform 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(25)SEG	This command was introduced.

Usage Guidelines	CFM is an end-to-end per-service-instance Ethernet layer operation, administration, and management (OAM) protocol that 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
	show debugging	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(25)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
	show debugging	Displays information about the types of debugging that are enabled.

debug platform cpu-queues

Use the **debug platform cpu-queues** privileged EXEC command to enable debugging of platform CPU receive queues. Use the **no** form of this command to disable debugging.

```
debug platform cpu-queues {broadcast-q | cbt-to-spt-q | cpuhub-q | host-q | icmp-q |
  igmp-snooping-q | layer2-protocol-q | logging-q | remote-console-q | routing-protocol-q |
  rpffail-q | software-fwd-q | stp-q}
```

```
no debug platform cpu-queues {broadcast-q | cbt-to-spt-q | cpuhub-q | host-q | icmp-q |
  igmp-snooping-q | layer2-protocol-q | logging-q | remote-console-q | routing-protocol-q |
  rpffail-q | software-fwd-q | stp-q}
```

Syntax Description		
broadcast-q		Display debug messages about packets received by the broadcast queue.
cbt-to-spt-q		Display debug messages about packets received by the core-based tree to shortest-path tree (cbt-to-spt) queue.
cpuhub-q		Display debug messages about packets received by the CPU heartbeat queue.
host-q		Display debug messages about packets received by the host queue.
icmp-q		Display debug messages about packets received by the Internet Control Message Protocol (ICMP) queue.
igmp-snooping-q		Display debug messages about packets received by the Internet Group Management Protocol (IGMP)-snooping queue.
layer2-protocol-q		Display debug messages about packets received by the Layer 2 protocol queue.
logging-q		Display debug messages about packets received by the logging queue.
remote-console-q		Display debug messages about packets received by the remote console queue.
routing-protocol-q		Display debug messages about packets received by the routing protocol queue.
rpffail-q		Display debug messages about packets received by the reverse path forwarding (RFP) failure queue.
software-fwd-q		Debug packets received by the software forwarding queue.
stp-q		Debug packets received by the Spanning Tree Protocol (STP) queue.

Defaults Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines The **undebg platform cpu-queues** command is the same as the **no debug platform cpu-queues** command.

 debug platform cpu-queues

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

debug platform dot1x

Use the **debug platform dot1x** privileged EXEC command to enable debugging of 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

initialization	Display 802.1x initialization sequence debug messages.
interface-configuration	Display 802.1x interface configuration-related debug messages.
rpc	Display 802.1x remote procedure call (RPC) request debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The **undebg platform dot1x** command is the same as the **no debug platform dot1x** command.

Related Commands

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

debug platform etherchannel

Use the **debug platform etherchannel** privileged EXEC command to enable debugging of platform-dependent EtherChannel events. Use the **no** form of this command to disable debugging.

debug platform etherchannel {init | link-up | rpc-detailed | rpc-generic | warnings}

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

Syntax Description

init	Display EtherChannel module initialization debug messages.
link-up	Display EtherChannel link-up and link-down related debug messages.
rpc-detailed	Display detailed EtherChannel remote procedure call (RPC) debug messages.
rpc-generic	Display EtherChannel RPC generic debug messages.
warnings	Display EtherChannel warning debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The **undebg platform etherchannel** command is the same as the **no debug platform etherchannel** command.

Related Commands

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

debug platform fallback-bridging

Use the **debug platform fallback-bridging** privileged EXEC command to enable debugging of the platform-dependent fallback bridging manager. Use the **no** form of this command to disable debugging.

debug platform fallback-bridging [**error** | **retry** | **rpc** {**events** | **messages**}]

no debug platform fallback-bridging [**error** | **retry** | **rpc** {**events** | **messages**}]

Syntax Description	error	(Optional) Display fallback bridging manager error condition debug messages.
	retry	(Optional) Display fallback bridging manager retry debug messages.
	rpc { events messages }	(Optional) Display fallback bridging debugging information. The keywords have these meanings:
		• events—Display remote procedure call (RPC) events. • messages—Display RPC messages.

Defaults	Debugging is disabled.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	If you do not specify a keyword, all fallback bridging manager debug messages are displayed. The undebg platform fallback-bridging command is the same as the no debug platform fallback-bridging command.

Related Commands	Command	Description
	show debugging	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

adjustment	(Optional) Display TCAM manager-adjustment debug messages.
allocate	(Optional) Display TCAM manager-allocation debug messages.
audit	(Optional) Display TCAM manager-audit debug messages.
error	(Optional) Display TCAM manager-error debug messages.
move	(Optional) Display TCAM manager-move debug messages.
read	(Optional) Display TCAM manager-read debug messages.
write	(Optional) Display TCAM manager-write debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

If you do not specify a keyword, all forwarding TCAM manager debug messages are displayed.

The **undebg platform forw-tcam** command is the same as the **no debug platform forw-tcam** command.

Related Commands

Command	Description
show debugging	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

all	Display all dynamic ARP inspection debug messages.
error	Display dynamic ARP inspection error debug messages.
event	Display dynamic ARP inspection event debug messages.
packet	Display dynamic ARP inspection packet-related debug messages.
rpc	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(25)EY	This command was introduced.

Usage Guidelines

The **undebg platform ip arp inspection** command is the same as the **no debug platform ip arp inspection** command.

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

Related Commands

Command	Description
show ip arp inspection	Displays the dynamic ARP inspection configuration and operating state.
show debugging	Displays information about the types of debugging that are enabled.

debug platform ip igmp snooping

Use the **debug platform ip igmp snooping** privileged EXEC command to enable debugging of platform-dependent Internet Group Management Protocol (IGMP) snooping. Use the **no** form of this command to disable debugging.

debug platform ip igmp snooping { **all** | **di** | **error** | **event** | **group** | **mgmt** | **pak** | **retry** | **rpc** | **warn** }

debug platform ip igmp snooping di [**grant** | **leave** | **rx** | **sync** | **tx** | **ucast**]

debug platform ip igmp snooping pak { *ip-address* | **error** | **ipopt** | **leave** | **query** | **report** | **rx** | **svi** | **tx** }

debug platform ip igmp snooping rpc [**cfg** | **I3mm** | **misc** | **vlan**]

no debug platform ip igmp snooping { **all** | **di** | **error** | **event** | **group** | **mgmt** | **pak** | **retry** | **rpc** | **warn** }

Syntax Description

all	Display all IGMP snooping debug messages.
di	Display IGMP snooping destination index (DI) coordination remote procedure call (RPC) debug messages. grant—(Optional) Display all IGMP snooping grant request RPC events. leave—(Optional) Display all IGMP snooping leave request RPC events. rx—(Optional) Display all IGMP snooping DI receive RPC messages. sync—(Optional) Display all IGMP snooping DI sync update messages. tx—(Optional) Display all IGMP snooping DI sent RPC messages. ucast—(Optional) Display all IGMP snooping DI unicast request RPC messages.
error	Display IGMP snooping error messages.
event	Display IGMP snooping event debug messages.
group	Display IGMP snooping group debug messages.
mgmt	Display IGMP snooping management debug messages.
pak { <i>ip-address</i> error ipopt leave query report rx svi tx }	Display IGMP snooping packet event debug messages. The keywords have these meanings: <i>ip-address</i>—IP address of the IGMP group. error—Display IGMP snooping packet error debug messages. ipopt—Display IGMP snooping IP bridging options debug messages. leave—Display IGMP snooping leave debug messages. query—Display IGMP snooping query debug messages. report—Display IGMP snooping report debug messages. rx—Display IGMP snooping received packet debug messages. svi—Display IGMP snooping switched virtual interface (SVI) packet debug messages. tx—Display IGMP snooping sent packet debug messages.

retry	Display IGMP snooping retry debug messages.
rpc [cfg l3mm misc vlan]	Display IGMP snooping remote procedure call (RPC) event debug messages. The keywords have these meanings: cfg—(Optional) Display IGMP snooping RPC debug messages. l3mm—(Optional) IGMP snooping Layer 3 multicast router group RPC debug messages. misc—(Optional) IGMP snooping miscellaneous RPC debug messages. vlan—(Optional) IGMP snooping VLAN assert RPC debug messages.
warn	Display IGMP snooping warning messages.

Defaults Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	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
	debug ip igmp snooping	Displays information about platform-independent IGMP snooping activity.
	show debugging	Displays information about the types of debugging that are enabled.

debug platform 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 { **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 { **all** | **mdb** | **mdfs-rp-retry** | **midb** | **mroute-rp** | **resources** | **retry** | **rpf-throttle** | **snoop-events** | **software-forward** | **swidb-events** | **vlan-locks** }

Syntax Description		
all	Display all platform IP-multicast event debug messages.	Note Using this command can degrade the performance of the switch.
mdb	Display IP-multicast debug messages for multicast distributed fast switching (MDFS) multicast descriptor block (mdb) events.	
mdfs-rp-retry	Display IP-multicast MDFS rendezvous point (RP) retry event debug messages.	
midb	Display IP-multicast MDFS multicast interface descriptor block (MIDB) debug messages.	
mroute-rp	Display IP-multicast RP event debug messages.	
resources	Display IP-multicast hardware resource debug messages.	
retry	Display IP-multicast retry processing event debug messages.	
rpf-throttle	Display IP-multicast reverse path forwarding (RPF) throttle event debug messages.	
snoop-events	Display IP-multicast IGMP snooping event debug messages.	
software-forward	Display IP-multicast software forwarding event debug messages.	
swidb-events	Display IP-multicast MDFS software interface descriptor block (swidb) or global event debug messages.	
vlan-locks	Display IP-multicast VLAN lock and unlock event debug messages.	

Defaults Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

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

Related Commands

Command	Description
show debugging	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

adjacency	Display IP unicast routing adjacency programming event debug messages.
all	Display all platform IP unicast routing debug messages. Note Using this command can degrade the performance of the switch.
arp	Display IP unicast routing Address Resolution Protocol (ARP) and ARP throttling debug messages.
dhcp	Display IP unicast routing DHCP dynamic address-related event debug messages.
errors	Display all IP unicast routing error debug messages, including resource allocation failures.
events	Display all IP unicast routing event debug messages, including registry and miscellaneous events.
interface	Display IP unicast routing interface event debug messages.
mpath	Display IP unicast routing multi-path adjacency programming event debug messages (present when performing equal or unequal cost routing).
registries	Display IP unicast routing forwarding information database (FIB), adjacency add, update, and delete registry event debug messages.
retry	Display IP unicast routing reprogram FIBs with ternary content addressable memory (TCAM) allocation failure debug messages.
route	Display IP unicast routing FIB TCAM programming event debug messages.
rpc	Display IP unicast routing Layer 3 unicast remote procedure call (RPC) interaction debug messages.
standby	Display IP unicast routing standby event debug messages, helpful in troubleshooting Hot Standby Routing Protocol (HSRP) issues.
statistics	Display IP unicast routing statistics gathering-related event debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The **undebg platform ip unicast** command is the same as the **no debug platform ip unicast** command.

Related Commands

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

debug platform led

Use the **debug platform led** privileged EXEC command to enable debugging of LED actions. Use the **no** form of this command to disable debugging.

debug platform led {generic | signal}

no debug platform led {generic | signal}

Syntax Description

generic	Display LED generic action debug messages.
signal	Display LED signal bit map debug messages.



Note

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
12.1(14)AX	This command was introduced.

Usage Guidelines

The **undebbug platform led** command is the same as the **no debug platform led** command.

Related Commands

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

debug platform matm

Use the **debug platform matm** privileged EXEC command to enable debugging of platform-dependent MAC address management. Use the **no** form of this command to disable debugging.

debug platform matm {aging | all | ec-aging | errors | learning | rpc | secure-address | warnings}

no debug platform matm {aging | all | ec-aging | errors | learning | rpc | secure-address | warnings}

Syntax Description

aging	Display MAC address aging debug messages.
all	Display all platform MAC address management event debug messages.
ec-aging	Display EtherChannel address aging-related debug messages.
errors	Display MAC address management error debug messages.
learning	Display MAC address management address-learning debug messages.
rpc	Display MAC address management remote procedure call (RPC) related debug messages.
secure-address	Display MAC address management secure address learning debug messages.
warning	Display MAC address management warning debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The **undebug platform matm** command is the same as the **no debug platform matm** command.

Related Commands

Command	Description
debug matm	Displays information about platform-independent MAC address management.
show debugging	Displays information about the types of debugging that are enabled.

debug platform messaging application

Use the **debug platform messaging application** privileged EXEC command to enable debugging of application messaging activity. Use the **no** form of this command to disable debugging.

debug platform messaging application { **all** | **badpak** | **cleanup** | **events** | **memerr** | **messages** | **usererr** }

no debug platform messaging application { **all** | **badpak** | **cleanup** | **events** | **memerr** | **messages** | **usererr** }

Syntax Description

all	Display all application-messaging debug messages.
badpak	Display bad-packet debug messages.
cleanup	Display clean-up debug messages.
events	Display event debug messages.
memerr	Display memory-error debug messages.
messages	Display application-messaging debug messages.
usererr	Display user-error debug messages.



Note

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
12.1(14)AX	This command was introduced.

Usage Guidelines

The **undebg platform messaging application** command is the same as the **no debug platform messaging application** command.

Related Commands

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

debug platform mpls

Use the **debug platform mpls** privileged EXEC command to enable debugging of the multiprotocol label switching (MPLS) control layer. Use the **no** form of this command to disable debugging.

debug platform mpls { **backwalk** | **encaps** | **errors** | **events** | **lspv** | **np** | **timer** }

no debug platform mpls { **backwalk** | **encaps** | **errors** | **events** | **lspv** | **np** | **timer** }

Syntax Description	backwalk	Display MPLS backwalk messages.
	encaps	Display MPLS encapsulation messages.
	errors	Display MPLS error messages.
	events	Display all MPLS event messages.
	lspv	Display MPLS label-switched path verification (LSPV) messages.
	np	Display MPLS network processor (NP) messages.
	timer	Display MPLS timer messages.

Defaults	Debugging is disabled.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.2(37)SE	This command was introduced.

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

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

debug platform phy

Use the **debug platform phy** privileged EXEC command to enable debugging of PHY driver information. Use the **no** form of this command to disable debugging.

debug platform phy {**automdix** | **flowcontrol** | **forced** | **init-seq** | **link-status** | **read** | **sfp** | **show-controller** | **speed** | **write**}

no debug platform phy {**automdix** | **flowcontrol** | **forced** | **init-seq** | **link-status** | **read** | **sfp** | **show-controller** | **speed** | **write**}

Syntax Description

automdix	Display PHY automatic medium-dependent-interface crossover (Auto-MDIX) debug messages.
flowcontrol	Display PHY flowcontrol debug messages.
forced	Display PHY forced-mode debug messages.
init-seq	Display PHY initialization-sequence debug messages.
link-status	Display PHY link-status debug messages.
read	Display PHY-read debug messages.
sfp	Display PHY small form-factor pluggable (SFP) modules debug messages.
show-controller	Display PHY show-controller debug messages.
speed	Display PHY speed-change debug messages.
write	Display PHY-write debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The **undebg platform phy** command is the same as the **no debug platform phy** command.

Related Commands

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

debug platform pm

Use the **debug platform pm** privileged EXEC command to enable debugging of the platform-dependent port manager software module. Use the **no** form of this command to disable debugging.

debug platform pm { **all** | **atom** | **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** | **vlangs** }

no debug platform pm { **all** | **atom** | **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** | **vlangs** }

Syntax Description	
all	Display all port-manager debug messages.
atom	Display port manager Any Transport over MPLS (AToM) related debug messages.
counters	Display counters for remote procedure call (RPC) debug messages.
errdisable	Display error-disabled related-events debug messages.
etherchnl	Display EtherChannel related-events debug messages.
exceptions	Display system exception debug messages.
hpm-events	Display platform port-manager event debug messages.
idb-events	Display interface descriptor block (IDB) related-events debug messages.
if-numbers	Display interface-number translation-event debug messages.
ios-events	Display Cisco IOS event debug messages.
link-status	Display interface link-detection event debug messages.
platform	Display port-manager function-event debug messages.
pm-events	Display port manager event debug messages.
pm-vectors [detail]	Display port-manager vector-related-event debug messages. The keyword has this meaning: detail—Display vector-function details.
rpc [general oper-info state vectors vp-events]	Display RPC related-event debug messages. The keywords have these meanings: general—(Optional) Display RPC general events. oper-info—(Optional) Display operational- and informational-related RPC messages. state—(Optional) Display administrative- and operational-related RPC messages. vectors—(Optional) Display vector-related RPC messages. vp-events—(Optional) Display virtual ports related-events RP messages.
soutput	Display IDB output vector event debug messages.
sync	Display operational synchronization and VLAN line-state event debug messages.
vlangs	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
12.1(14)AX	This command was introduced.

Usage Guidelines

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

Related Commands

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

debug platform port-asic

Use the **debug platform port-asic** privileged EXEC command to enable debugging of the port application-specific integrated circuit (ASIC) driver. Use the **no** form of this command to disable debugging.

debug platform port-asic {**interrupt** | **periodic** | **read** | **write**}

no debug platform port-asic {**interrupt** | **periodic** | **read** | **write**}

Syntax Description

interrupt	Display port-ASIC interrupt-related function debug messages.
periodic	Display port-ASIC periodic-function-call debug messages.
read	Display port-ASIC read debug messages.
write	Display port-ASIC write 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
12.1(14)AX	This command was introduced.

Usage Guidelines

The **undebug platform port-asic** command is the same as the **no debug platform port-asic** command.

Related Commands

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

debug platform 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

add	Display secure address addition debug messages.
aging	Display secure address aging debug messages.
all	Display all port-security debug messages.
delete	Display secure address deletion debug messages.
errors	Display port-security error debug messages.
rpc	Display remote procedure call (RPC) debug messages.
warnings	Display warning debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The **undebug platform port-security** command is the same as the **no debug platform port-security** command.

Related Commands

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

debug platform qos-acl-tcam

Use the **debug platform qos-acl-tcam** privileged EXEC command to enable debugging of the quality of service (QoS) and access control list (ACL) 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 | rpc | tcam}

no debug platform qos-acl-tcam {all | ctcam | errors | labels | mask | rpc | tcam}

Syntax Description

all	Display all QoS and ACL TCAM (QATM) manager debug messages.
ctcam	Display Cisco TCAM (CTCAM) related-events debug messages.
errors	Display QATM error-related-events debug messages.
labels	Display QATM label-related-events debug messages.
mask	Display QATM mask-related-events debug messages.
rpc	Display QATM remote procedure call (RPC) related-events debug messages.
tcam	Display QATM TCAM-related events debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The **undebg platform qos-acl-tcam** command is the same as the **no debug platform qos-acl-tcam** command.

Related Commands

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

debug platform 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
	12.1(14)AX	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
	show debugging	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(40)SE	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
	show debugging	Displays information about the types of debugging that are enabled.

debug platform resource-manager

Use the **debug platform resource-manager** privileged EXEC command to enable debugging of the resource manager software. Use the **no** form of this command to disable debugging.

debug platform resource-manager { **all** | **dm** | **erd** | **errors** | **madmed** | **sd** | **stats** | **vld** }

no debug platform resource-manager { **all** | **dm** | **erd** | **errors** | **madmed** | **sd** | **stats** | **vld** }

Syntax Description

all	Display all resource manager debug messages.
dm	Display destination-map debug messages.
erd	Display equal-cost-route descriptor-table debug messages.
errors	Display error debug messages.
madmed	Display the MAC address descriptor table and multi-expansion descriptor table debug messages.
sd	Display the station descriptor table debug messages.
stats	Display statistics debug messages.
vld	Display the VLAN-list descriptor debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The **undebg platform resource-manager** command is the same as the **no debug platform resource-manager** command.

Related Commands

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

debug platform snmp

Use the **debug platform snmp** privileged EXEC command to enable debugging of the platform-dependent Simple Network Management Protocol (SNMP) software. Use the **no** form of this command to disable debugging.

debug platform snmp

no debug platform snmp

Syntax Description	This command has no arguments or keywords.

Defaults	Debugging is disabled.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	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
	show debugging	Displays information about the types of debugging that are enabled.

debug platform span

Use the **debug platform span** privileged EXEC command to enable debugging of the platform-dependent Switched Port Analyzer (SPAN) software. Use the **no** form of this command to disable debugging.

debug platform span

no debug platform span

Syntax Description	This command has no arguments or keywords.

Defaults	Debugging is disabled.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	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
	show debugging	Displays information about the types of debugging that are enabled.

debug platform supervisor-asic

Use the **debug platform supervisor-asic** privileged EXEC command to enable debugging of the supervisor application-specific integrated circuit (ASIC). Use the **no** form of this command to disable debugging.

debug platform supervisor-asic {all | errors | receive | send}

no debug platform supervisor-asic {all | errors | receive | send}

Syntax Description

all	Display all supervisor-ASIC event debug messages.
errors	Display the supervisor-ASIC error debug messages.
receive	Display the supervisor-ASIC receive debug messages.
send	Display the supervisor-ASIC send debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The **undebug platform supervisor-asic** command is the same as the **no debug platform supervisor-asic** command.

Related Commands

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

debug platform sw-bridge

Use the **debug platform sw-bridge** privileged EXEC command to enable debugging of the software bridging function. Use the **no** form of this command to disable debugging.

debug platform sw-bridge { **broadcast** | **control** | **multicast** | **packet** | **unicast** }

no debug platform sw-bridge { **broadcast** | **control** | **multicast** | **packet** | **unicast** }

Syntax Description

broadcast	Display broadcast-data debug messages.
control	Display protocol-packet debug messages.
multicast	Display multicast-data debug messages.
packet	Display sent and received data debug messages.
unicast	Display unicast-data debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The **undebug platform sw-bridge** command is the same as the **no debug platform sw-bridge** command.

Related Commands

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

debug platform tcam

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} | ipv6 {acl {input | output} | local | qos |  
secondary} | 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} | ipv6 {acl {input | output} | local | qos |  
secondary} | 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

log l2 {acl {input output} local qos}	Display Layer-2 field-based CAM look-up type debug messages. The keywords have these meanings: • acl {input output}—Display input or output ACL look-up debug messages. • local—Display local forwarding look-up debug messages. • qos—Display classification and quality of service (QoS) look-up debug messages.

debug platform tcam

l3 { acl { input output } ipv6 { acl { input output } local qos secondary } local qos secondary }	Display Layer-3 field-based CAM look-up type debug messages. The keywords have these meanings: • acl {input output}—Display input or output ACL look-up debug messages. • ipv6 {acl {input output} local qos secondary}—Display IPv6-based look-up debug messages. Options include displaying input or output ACL look-up, local forwarding look-up, classification and QoS look-up, or secondary forwarding look-up debug messages. • local—Display local forwarding look-up debug messages. • qos—Display classification and quality of service (QoS) look-up debug messages. • secondary—Display secondary forwarding look-up debug messages.
read { reg ssram tcam }	Display TCAM-read debug messages. The keywords have these meanings: • reg—Display TCAM-register read debug messages. • ssram—Display synchronous static RAM (SSRAM)-read debug messages. • tcam—Display TCAM-read debug messages.
search	Display supervisor-initiated TCAM-search results debug messages.
write { forw-ram reg tcam }	Display TCAM-write debug messages. The keywords have these meanings: forw-ram—Display forwarding-RAM write debug messages. reg—Display TCAM-register write debug messages. tcam—Display TCAM-write debug messages.

Defaults Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	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
	show debugging	Displays information about the types of debugging that are enabled.

debug platform uddld

Use the **debug platform uddld** 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 uddld [**all** | **error** | **rpc** {**events** | **messages**}]

no debug platform uddld [**all** | **error** | **rpc** {**events** | **messages**}]

Syntax Description

all	(Optional) Display all UDLD debug messages.
error	(Optional) Display error condition debug messages.
rpc { events messages }	(Optional) Display UDLD remote procedure call (RPC) debug messages. The keywords have these meanings: • events—Display UDLD RPC events. • messages—Display UDLD RPC messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The **undebg platform uddld** command is the same as the **no debug platform uddld** command.

Related Commands

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

debug platform vlan

Use the **debug platform vlan** privileged EXEC command to enable debugging of the VLAN manager software. Use the **no** form of this command to disable debugging.

debug platform vlan {errors | mvid | rpc}

no debug platform vlan {errors | mvid | rpc}

Syntax Description

errors	Display VLAN error debug messages.
mvid	Display mapped VLAN ID allocations and free debug messages.
rpc	Display remote procedure call (RPC) debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The **undebg platform vlan** command is the same as the **no debug platform vlan** command.

Related Commands

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

debug pm

Use the **debug pm privileged EXEC** command to enable debugging of port manager (PM) activity. The port manager is a state machine that controls all the logical and physical ports. 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		
all		Display all PM debug messages.
assert		Display assert debug messages.
card		Display line-card related-events debug messages.
cookies		Display internal PM cookie validation debug messages.
etherchnl		Display EtherChannel related-events debug messages.
hatable		Display Host Access Table events debug messages.
messages		Display PM debug messages.
port		Display port related-events debug messages.
registry		Display PM registry invocation debug messages.
sm		Display state-machine related-events debug messages.
span		Display spanning-tree related-events debug messages.
split		Display split-processor debug messages.
vlan		Display VLAN related-events debug messages.
vp		Display virtual port related-events debug messages.



Note

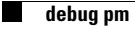
Though visible in the command-line help strings, the **scp** and **pvlan** keywords are not supported.

Defaults Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

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

**Related Commands**

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

debug 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
	12.1(14)AX	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
	show debugging	Displays information about the types of debugging that are enabled.
	show port-security	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** | **lslsm** | **packet** | **prsm** }

no debug rep { **all** | **bpa-event** | **bpasm** | **epasm** | **error** | **failure-recovery** | **lslsm** | **packet** | **prsm** }

Syntax Description

all	Display all REP debug messages.
bpa-event	Display blocked port advertisement (BPA) debug messages.
bpasm	Display BPA state machine debug messages.
epasm	Display end port advertisement (EPA) state machine debug messages.
error	Display REP protocol error debug messages.
failure-recovery	Display REP switchover event debug messages.
lslsm	Display Link State Layer (LSL) state machine debug messages.
packet	Display protocol PDU debug messages.
prsm	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
show debugging	Displays information about the types of debugging that are enabled.
show interfaces rep	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
12.1(14)AX	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 | backbonefast | bpdu | bpdu-opt | config | etherchannel | events |
exceptions | general | mstp | pvst+ | root | snmp | switch | synchronization | uplinkfast}
```

```
no debug spanning-tree {all | backbonefast | bpdu | bpdu-opt | config | etherchannel | events |
exceptions | general | mstp | pvst+ | root | snmp | switch | synchronization | uplinkfast}
```

Syntax Description

all	Display all spanning-tree debug messages.
backbonefast	Display BackboneFast-event debug messages.
bpdu	Display spanning-tree bridge protocol data unit (BPDU) debug messages.
bpdu-opt	Display optimized BPDU handling debug messages.
config	Display spanning-tree configuration change debug messages.
etherchannel	Display EtherChannel-support debug messages.
events	Display spanning-tree topology event debug messages.
exceptions	Display spanning-tree exception debug messages.
general	Display general spanning-tree activity debug messages.
mstp	Debug Multiple Spanning Tree Protocol events.
pvst+	Display per-VLAN spanning-tree plus (PVST+) event debug messages.
root	Display spanning-tree root-event debug messages.
snmp	Display spanning-tree Simple Network Management Protocol (SNMP) handling debug messages.
synchronization	Display the spanning-tree synchronization event debug messages.
switch	Display switch shim command debug messages. This shim is the software module that is the interface between the generic Spanning Tree Protocol (STP) code and the platform-specific code of various switch platforms.
uplinkfast	Display UplinkFast-event debug messages.



Note

Though visible in the command-line help strings, the **csuf/csrt** keyword is not supported.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	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
show debugging	Displays information about the types of debugging that are enabled.
show spanning-tree	Displays spanning-tree state information.

debug spanning-tree backbonefast

Use the **debug spanning-tree backbonefast** privileged EXEC command to enable debugging of spanning-tree BackboneFast events. Use the **no** form of this command to disable debugging.

debug spanning-tree backbonefast [detail | exceptions]

no debug spanning-tree backbonefast [detail | exceptions]

Syntax Description	detail	(Optional) Display detailed BackboneFast debug messages.
	exceptions	(Optional) Display spanning-tree BackboneFast-exception debug messages.
Defaults	Debugging is disabled.	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	12.1(14)AX	This command was introduced.
Usage Guidelines	The undebg spanning-tree backbonefast command is the same as the no debug spanning-tree backbonefast command.	
Related Commands	Command	Description
	show debugging	Displays information about the types of debugging that are enabled.
	show spanning-tree	Displays spanning-tree state information.

debug spanning-tree bpdud

Use the **debug spanning-tree bpdud** 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 bpdud [receive | transmit]

no debug spanning-tree bpdud [receive | transmit]

Syntax Description

receive	(Optional) Display the nonoptimized path for received BPDU debug messages.
transmit	(Optional) Display the nonoptimized path for transmitted BPDU debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The **undebud spanning-tree bpdud** command is the same as the **no debug spanning-tree bpdud** command.

Related Commands

Command	Description
show debudding	Displays information about the types of debudding that are enabled.
show spanning-tree	Displays spanning-tree state information.

debug spanning-tree bpdu-opt

Use the **debug spanning-tree bpdu-opt** privileged EXEC command to enable debugging of optimized spanning-tree bridge protocol data units (BPDUs) handling. Use the **no** form of this command to disable debugging.

debug spanning-tree bpdu-opt [**detail** | **packet**]

no debug spanning-tree bpdu-opt [**detail** | **packet**]

Syntax Description	detail	(Optional) Display detailed optimized BPDU-handling debug messages.
	packet	(Optional) Display packet-level optimized BPDU-handling debug messages.

Defaults	Debugging is disabled.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	The undebbug spanning-tree bpdu-opt command is the same as the no debug spanning-tree bpdu-opt command.

Related Commands	Command	Description
	show debugging	Displays information about the types of debugging that are enabled.
	show spanning-tree	Displays spanning-tree state information.

debug spanning-tree mstp

Use the **debug spanning-tree mstp** privileged EXEC command to enable debugging of the Multiple Spanning Tree Protocol (MSTP) software. Use the **no** form of this command to disable debugging.

```
debug spanning-tree mstp {all | boundary | bpdu-rx | bpdu-tx | errors | flush | init | migration |
pm | proposals | region | roles | sanity_check | sync | tc | timers}
```

```
no debug spanning-tree mstp {all | boundary | bpdu-rx | bpdu-tx | errors | flush | init | migration
| pm | proposals | region | roles | sanity_check | sync | tc | timers}
```

Syntax Description	
all	Display all MSTP debug messages.
boundary	Display flag change debug messages at these boundaries: - An multiple spanning-tree (MST) region and a single spanning-tree region running Rapid Spanning Tree Protocol (RSTP) - An MST region and a single spanning-tree region running 802.1D - An MST region and another MST region with a different configuration
bpdu-rx	Display received MST bridge protocol data unit (BPDUs) debug messages.
bpdu-tx	Display sent MST BPDU debug messages.
errors	Display MSTP error debug messages.
flush	Display port-flushing mechanism debug messages.
init	Display MSTP data structure initialization debug messages.
migration	Display protocol-migration state-machine debug messages.
pm	Display MSTP port-manager event debug messages.
proposals	Display handshake messages between the designated switch and the root switch debug messages.
region	Display region synchronization between the switch processor (SP) and the route processor (RP) debug messages.
roles	Display MSTP role debug messages.
sanity_check	Display received BPDU sanity check debug messages.
sync	Display port synchronization event debug messages.
tc	Display topology change notification event debug messages.
timers	Display MSTP timers for start, stop, and expire event debug messages.

Defaults Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

debug spanning-tree mstp**Usage Guidelines**

The **undebbug spanning-tree mstp** command is the same as the **no debug spanning-tree mstp** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show spanning-tree	Displays spanning-tree state information.

debug spanning-tree switch

Use the **debug spanning-tree switch privileged EXEC** command to enable debugging of the software interface between the Spanning Tree Protocol (STP) software module and the port manager software module. Use the **no** form of this command to disable debugging.

debug spanning-tree switch { **all** | **errors** | **flush** | **general** | **helper** | **pm** | **rx** { **decode** | **errors** | **interrupt** | **process** } | **state** | **tx** [**decode**] | **uplinkfast** }

no debug spanning-tree switch { **all** | **errors** | **flush** | **general** | **helper** | **pm** | **rx** { **decode** | **errors** | **interrupt** | **process** } | **state** | **tx** [**decode**] | **uplinkfast** }

Syntax Description		
all		Display all spanning-tree switch debug messages.
errors		Display debug messages for the interface between the spanning-tree software module and the port manager software module.
flush		Display shim flush operation debug messages.
general		Display general event debug messages.
helper		Display spanning-tree helper-task debug messages. Helper tasks handle bulk spanning-tree updates.
pm		Display port-manager event debug messages.
rx		Display received bridge protocol data unit (BPDU) handling debug messages. The keywords have these meanings: decode—Display decoded received packets. errors—Display receive error debug messages. interrupt—Display interrupt service request (ISR) debug messages. process—Display process receive BPDU debug messages.
state		Display spanning-tree port state change debug messages.
tx [decode]		Display transmitted BPDU handling debug messages. The keyword has this meaning: decode—(Optional) Display decoded transmitted packets.
uplinkfast		Display uplinkfast packet transmission debug messages.

Defaults Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

 debug spanning-tree switch**Usage Guidelines**

The **undebg spanning-tree switch** command is the same as the **no debug spanning-tree switch** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show spanning-tree	Displays spanning-tree state information.

debug spanning-tree uplinkfast

Use the **debug spanning-tree uplinkfast privileged EXEC** command to enable debugging of spanning-tree UplinkFast events. Use the **no** form of this command to disable debugging.

debug spanning-tree uplinkfast [exceptions]

no debug spanning-tree uplinkfast [exceptions]

Syntax Description	exceptions (Optional) Display spanning-tree UplinkFast-exception debug messages.	
Defaults	Debugging is disabled.	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	12.1(14)AX	This command was introduced.
Usage Guidelines	The undebg spanning-tree uplinkfast command is the same as the no debug spanning-tree uplinkfast command.	
Related Commands	Command	Description
	show debugging	Displays information about the types of debugging that are enabled.
	show spanning-tree	Displays spanning-tree state information.

debug sw-vlan

Use the **debug sw-vlan** privileged EXEC command to enable debugging of VLAN manager activities. Use the **no** form of this command to disable debugging.

debug sw-vlan { **badpmcookies** | **cfg-vlan** { **bootup** | **cli** } | **events** | **ifs** | **management** | **notification** | **packets** | **registries** | **vtp** }

no debug sw-vlan { **badpmcookies** | **cfg-vlan** { **bootup** | **cli** } | **events** | **ifs** | **management** | **notification** | **packets** | **registries** | **vtp** }

Syntax Description	
badpmcookies	Display VLAN manager incidents of bad port manager cookie debug messages.
cfg-vlan { bootup cli }	Display config-vlan debug messages. The keywords have these meanings: bootup—Display messages when the switch is booting up. cli—Display messages when the command-line interface (CLI) is in config-vlan mode.
events	Display VLAN manager event debug messages.
ifs	See the debug sw-vlan ifs command.
management	Display VLAN manager management of internal VLAN debug messages.
notification	See the debug sw-vlan notification command.
packets	Display packet handling and encapsulation process debug messages.
registries	Display VLAN manager registry debug messages.
vtp	See the debug sw-vlan vtp command.

Defaults Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines The **undebug sw-vlan** command is the same as the **no debug sw-vlan** command.

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

Command	Description
<code>show vlan</code>	Displays the parameters for all configured VLANs or one VLAN (if the VLAN name or ID is specified) in the administrative domain.
<code>show vtp</code>	Displays general information about VTP management domain, status, and counters.

debug sw-vlan ifs

Use the **debug sw-vlan ifs** privileged EXEC command to enable debugging of the VLAN manager Cisco IOS file system (IFS) error tests. Use the **no** form of this command to disable debugging.

```
debug sw-vlan ifs {open {read | write} | read {1 | 2 | 3 | 4} | write}
```

```
no debug sw-vlan ifs {open {read | write} | read {1 | 2 | 3 | 4} | write}
```

Syntax Description

open {read write}	Display VLAN manager IFS file-open operation debug messages. The keywords have these meanings: read—Display VLAN manager IFS file-read operation debug messages. write—Display VLAN manager IFS file-write operation debug messages.
read {1 2 3 4}	Display file-read operation debug messages for the specified error test (1, 2, 3, or 4).
write	Display file-write operation debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The **undebug sw-vlan ifs** command is the same as the **no debug sw-vlan ifs** command.

When determining the file read operation, Operation **1** reads the file header, which contains the header verification word and the file version number. Operation **2** reads the main body of the file, which contains most of the domain and VLAN information. Operation **3** reads type length version (TLV) descriptor structures. Operation **4** reads TLV data.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN name or ID is specified) in the administrative domain.

debug sw-vlan notification

Use the **debug sw-vlan notification privileged EXEC** command to enable debugging of the activation and deactivation of Inter-Link Switch (ISL) VLAN IDs. Use the **no** form of this command to disable debugging.

debug sw-vlan notification { accfwdchange | allowedvlanfgchange | fwdchange | linkchange | modechange | pruningcfgchange | statechange }

no debug sw-vlan notification { accfwdchange | allowedvlanfgchange | fwdchange | linkchange | modechange | pruningcfgchange | statechange }

Syntax Description		
accfwdchange		Display debug messages for VLAN manager notification of aggregated access interface spanning-tree forward changes.
allowedvlanfgchange		Display debug messages for VLAN manager notification of changes to the allowed VLAN configuration.
fwdchange		Display debug messages for VLAN manager notification of spanning-tree forwarding changes.
linkchange		Display debug messages for VLAN manager notification of interface link-state changes.
modechange		Display debug messages for VLAN manager notification of interface mode changes.
pruningcfgchange		Display debug messages for VLAN manager notification of changes to the pruning configuration.
statechange		Display debug messages for VLAN manager notification of interface state changes.

Defaults Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines The **undebg sw-vlan notification** command is the same as the **no debug sw-vlan notification** command.

Related Commands	Command	Description
	show debugging	Displays information about the types of debugging that are enabled.
	show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN name or ID is specified) in the administrative domain.

debug sw-vlan vtp

Use the **debug sw-vlan vtp** privileged EXEC command to enable debugging of the VLAN Trunking Protocol (VTP) code. Use the **no** form of this command to disable debugging.

debug sw-vlan vtp { **events** | **packets** | **pruning** [**packets** | **xmit**] | **xmit** }

no debug sw-vlan vtp { **events** | **packets** | **pruning** | **xmit** }

Syntax Description		
	events	Display debug messages for general-purpose logic flow and detailed VTP messages generated by the VTP_LOG_RUNTIME macro in the VTP code.
	packets	Display debug messages for the contents of all incoming VTP packets that have been passed into the VTP code from the Cisco IOS VTP platform-dependent layer, except for pruning packets.
	pruning [packets xmit]	Display debug messages generated by the pruning segment of the VTP code. The keywords have these meanings: • packets—(Optional) Display debug messages for the contents of all incoming VTP pruning packets that have been passed into the VTP code from the VTP platform-dependent layer. • xmit—(Optional) Display debug messages for the contents of all outgoing VTP packets that the VTP code requests the Cisco IOS VTP platform-dependent layer to send.
	xmit	Display debug messages for the contents of all outgoing VTP packets that the VTP code requests the VTP platform-dependent layer to send, except for pruning packets.

Defaults Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines The **undebug sw-vlan vtp** command is the same as the **no debug sw-vlan vtp** command.

If no further parameters are entered after the **pruning** keyword, VTP pruning debugging messages are displayed. They are generated by the VTP_PRUNING_LOG_NOTICE, VTP_PRUNING_LOG_INFO, VTP_PRUNING_LOG_DEBUG, VTP_PRUNING_LOG_ALERT, and VTP_PRUNING_LOG_WARNING macros in the VTP pruning code.

Related Commands	Command	Description
	show debugging	Displays information about the types of debugging that are enabled.
	show vtp	Displays general information about VTP management domain, status, and counters.

debug 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

events	Display debug messages for UDLD process events as they occur.
packets	Display debug messages for the UDLD process as it receives packets from the packet queue and tries to send them at the request of the UDLD protocol code.
registries	Display debug messages for the UDLD process as it processes registry calls from the UDLD process-dependent module and other feature modules.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The **undebg udd** command is the same as the **no debug udd** command.

For **debug udd events**, these debugging messages are displayed:

- 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 are displayed:

- 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 are displayed:

- Sub-block creation
- Fiber-port status changes

- State change indications from the port manager software
- MAC address registry calls

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show udd	Displays UDD administrative and operational status for all ports or the specified port.

debug vqpc

Use the **debug vqpc** privileged EXEC command to enable debugging of the VLAN Query Protocol (VQP) client. Use the **no** form of this command to disable debugging.

debug vqpc [**all** | **cli** | **events** | **learn** | **packet**]

no debug vqpc [**all** | **cli** | **events** | **learn** | **packet**]

Syntax Description	all	(Optional) Display all VQP client debug messages.
	cli	(Optional) Display the VQP client command-line interface (CLI) debug messages.
	events	(Optional) Display VQP client event debug messages.
	learn	(Optional) Display VQP client address learning debug messages.
	packet	(Optional) Display VQP client packet information debug messages.

Defaults Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

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

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

debug xconnect

Use the **debug xconnect** privileged EXEC command to enable debugging of Layer 2 transport routing using Ethernet over multiprotocol label switching (EoMPLS). Use the **no** form of this command to disable debugging.

debug xconnect {error | event}

no debug xconnect {error | event}

Syntax Description

error	Display xconnect authorization error debug messages.
event	Display xconnect authorization event debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

The **undebg xconnect** command is the same as the **no debug xconnect** command.

Related Commands

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

■ debug xconnect



APPENDIX **C**

Catalyst 3750 Metro Switch Show Platform Commands

This appendix describes the **show platform** privileged EXEC commands that have been created or changed for use with the Catalyst 3750 Metro 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 | vlan vlan-id} [ | {begin | exclude | include} expression]
```

Syntax Description

interface <i>interface-id</i>	Display per-interface ACL manager information for the specified interface. The interface can be a physical interface, a port-channel, or a VLAN.
label <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: detail—(Optional) Display detailed ACL manager label information.
statistics <i>asic-number</i>	Display per-ASIC ACL manager information. The <i>asic-number</i> is the port ASIC number, either 0 or 1.
usage <i>asic-number</i>	Display per-ASIC ACL manager usage information. The <i>asic-number</i> is the port ASIC number, either 0 or 1.
vlan <i>vlan-id</i>	Display per-VLAN ACL manager information. The <i>vlan-id</i> range is from 1 to 4094.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

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

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 [**|** { **begin** | **exclude** | **include** } *expression*]

Syntax Description	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.2(25)SEG	This command was introduced.

Usage Guidelines	You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so. Expressions are case sensitive. For example, if you enter exclude output, the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

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} [ | {begin | exclude |
include} expression]
```

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.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

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

show platform etherchannel

Use the **show platform etherchannel** privileged EXEC command to display platform-dependent EtherChannel information.

show platform etherchannel {**flags** | **time-stamps**} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

flags	Display EtherChannel port flags.
time-stamps	Display EtherChannel time stamps.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

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

show platform forward

Use the **show platform forward** privileged EXEC command for a port to determine 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 [dscp dscp] [frag field] { l4protocol-id | icmp icmp-type icmp-code |
```

```
igmp igmp-version igmp-type | tcp src-port dst-port flags | udp src-port dst-port } [ | { begin |
```

```
exclude | include } expression]
```

Syntax Description

<i>interface-id</i>	The input physical port, the port on which the packet comes in to the switch.
vlan <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.
sap	(Optional) Service access point (SAP) encapsulation type.
snap	(Optional) Subnetwork Access Protocol (SNAP) encapsulation type.
cos <i>cos</i>	(Optional) Class of service (CoS) value of the frame. The range is 0 to 7.
ip <i>src-ip</i> <i>dst-ip</i>	(Optional, but required for IP packets) Source and destination IP addresses in dotted decimal notation.
dscp <i>dscp</i>	(Optional) Differentiated Services Code Point (DSCP) field in the IP header. The range is 0 to 63.
frag <i>field</i>	(Optional) The IP fragment field for a fragmented IP packet. The range is 0 to 65535.
<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.
icmp <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.
igmp <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.
tcp <i>src-port</i> <i>dst-port</i> <i>flags</i>	Transmission Control Protocol (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.
udp <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.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **l exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples for examples of the **show platform forward** command output displays and what they mean, see the “Troubleshooting” chapter of the software configuration guide for this release.

show platform ip igmp snooping

Use the **show platform ip igmp snooping** privileged EXEC command to display platform-dependent Internet Group Management Protocol (IGMP) snooping information.

```
show platform ip igmp snooping {all | control [di] | counters | flood [vlan vlan-id] | group
ip-address | hardware | retry [count | local [count] | remote [count]]} [ | {begin | exclude |
include} expression]
```

Syntax Description		
all		Display all IGMP snooping platform IP multicast information.
control [di]		Display IGMP snooping control entries. The keyword has this meaning: di—(Optional) Display IGMP snooping control destination index entries.
counters		Display IGMP snooping counters.
flood [vlan vlan-id]		Display IGMP snooping flood information. The keyword has this meaning: vlan vlan-id—(Optional) Display flood information for the specified VLAN. The range is 1 to 4094.
group ip-address		Display the IGMP snooping multicast group information, where <i>ip-address</i> is the IP address of the group.
hardware		Display IGMP snooping information loaded into hardware.
retry [count local [count] remote [count]]		Display IGMP snooping retry information. The keywords have these meanings: count—(Optional) Display only the retry count. local—(Optional) Display local retry entries.
remote [count]		Display remote entries. The keyword has this meaning: count—(Optional) Display only the remote count.
 begin		(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude		(Optional) Display excludes lines that match the <i>expression</i> .
 include		(Optional) Display includes lines that match the specified <i>expression</i> .
expression		Expression in the output to use as a reference point.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **l exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

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 | |
mds | retry {mdb | mroute} | trace} [ | {begin | exclude | include} expression]
```

Syntax Description

acl-full-info	Display ACL-full multicast route information.
counters	Display IP multicast counters and statistics.
groups	Display IP multicast routes per group.
hardware [detail]	Display IP multicast routes loaded into hardware. The optional detail keyword is used to show port members in the destination index and route index.
interfaces	Display IP multicast interfaces.
mds	Display multicast distributed fast switching (MDFS) IP multicast routes.
retry {mdb mroute}	Display the IP multicast routes in the retry queue. The keywords have these meanings: mdb—Display the multicast routes in retry queue waiting for hardware. mroute—Display the multicast routes in the retry queue, waiting for the destination and route index.
trace	Display the IP multicast trace buffer.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

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

show platform ip policy

Use the **show platform ip policy** privileged EXEC command to display platform-dependent IP policy information.

```
show platform ip policy {interfaces | route-map [name]} [ | {begin | exclude | include}
expression]
```

Syntax Description	interfaces	Display IP policy interface information.
	route-map [name]	Display IP policy route-map information. The keyword has this meaning: <i>name</i>—(Optional) Display information for the specified route map.
	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so. Expressions are case sensitive. For example, if you enter exclude output, the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

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 [A.B.C.D] | cef-idb | counts | dhcp | failed {adjacency | arp
[A.B.C.D] | route} | mpaths | proxy | route [A.B.C.D] | standby | statistics | trace} [ | {begin
| exclude | include} expression]
```

Syntax Description	
adjacency [A.B.C.D]	Display the platform adjacency database. The keyword has this meaning: A.B.C.D—(Optional) Display adjacency information for the specified IP address.
cef-idb	Display platform information corresponding to Cisco Express Forwarding (CEF) interface descriptor block.
counts	Display the current counts for the Layer 3 unicast databases.
dhcp	Display the DHCP system dynamic addresses.
failed { adjacency arp [A.B.C.D] route }	Display the hardware resource failures. The keywords have these meanings: adjacency—Display the adjacency entries that failed to be programmed in hardware. arp—Display the Address Resolution Protocol (ARP) deletions because of failure and because of retries. A.B.C.D—(Optional) Prefix of the ARP entries to display. route—Display the route entries that failed to be programmed in hardware.
mpaths	Display the Layer 3 unicast routing multipath adjacency database.
proxy	Display entries for the proxy Address Resolution Protocol (ARP) database.
route [A.B.C.D]	Display the platform route database. The keyword has this meaning: A.B.C.D—(Optional) Display entries for the specified IP prefix.
standby	Display the platform standby information.
statistics	Display the Layer 3 unicast routing accumulated statistics.
trace	Display the platform event trace logs.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **l exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

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 [ | {begin | exclude | include} expression]
```

Syntax Description	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.
	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

show platform layer4op

Use the **show platform layer4op** privileged EXEC command to display platform-dependent Layer 4 operator information.

```
show platform layer4op {acl | pacl [port-asic] | qos [port-asic]} {and-or | map | or-and | vcu}
[ | {begin | exclude | include} expression]
```

Syntax Description	
acl	Display access control list (ACL) Layer 4 operators information.
pacl [port-asic]	Display port ACL Layer 4 operations information. The keyword has this meaning: <i>port-asic</i>—(Optional) Port ASIC number. The value can be 0 or 1.
qos [port-asic]	Display quality of service (QoS) Layer 4 operators information. The keyword has this meaning: <i>port-asic</i>—(Optional) QoS port ASIC number. The value can be 0 or 1.
and-or	Display AND-OR registers information.
map	Display select map information.
or-and	Display OR-AND registers information.
vcu	Display value compare unit (VCU) register information.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

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

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*]] [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description	aging-array	(Optional) Display the MAC address table aging array.
	hash-table	(Optional) Display the MAC address table hash table.
	mac-address <i>mac-address</i>	(Optional) Display the MAC address table MAC address information, where <i>mac-address</i> is the 48-bit hardware address.
	vlan <i>vlan-id</i>	(Optional) Display information for the specified VLAN. The range is 1 to 4094.
	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

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

show platform messaging

Use the **show platform messaging** privileged EXEC command to display platform-dependent application and performance message information.

show platform messaging { **application** [**incoming** | **outgoing** | **summary**] | **hiperf** [*class-number*] } [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description	
application [incoming outgoing summary]	Display application message information. The keywords have these meanings: • incoming—(Optional) Display only information about incoming application messaging requests. • outgoing—(Optional) Display only information about incoming application messaging requests. • summary—(Optional) Display summary information about all application messaging requests.
hiperf [<i>class-number</i>]	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.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

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

show platform monitor

Use the **show platform monitor** privileged EXEC command to display platform-dependent Switched Port Analyzer (SPAN) information.

show platform monitor [**session** *session-number*] [**|** { **begin** | **exclude** | **include** } *expression*]

Syntax Description

session <i>session-number</i>	(Optional) Display SPAN information for the specified SPAN session. The range is 1 to 66.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

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

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 [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so. Expressions are case sensitive. For example, if you enter exclude output, the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

show platform pm

Use the **show platform pm** privileged EXEC command to display platform-dependent port-manager information.

```
show platform pm {counters | group-masks | idbs {active-idbs | deleted-idbs} | if-numbers |
link-status | platform-block | port-info interface-id | vlan {info | line-state}
[ | {begin | exclude | include} expression]
```

Syntax Description

counters	Display module counters information.
group-masks	Display EtherChannel group masks information.
idbs {active-idbs deleted-idbs}	Display interface data block (IDB) information. The keywords have these meanings: active-idbs—Display active IDB information. deleted-idbs—Display deleted and leaked IDB information.
if-numbers	Display interface numbers information.
link-status	Display local port link status information.
platform-block	Display platform port block information.
port-info interface-id	Display port administrative and operation fields for the specified physical or port-channel interface.
vlan {info line-state}	Display platform VLAN information. The keywords have these meanings: info—Display information for active VLANs. line-state—Display line-state information.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.



Note

Though visible in the command-line help strings, the **stack-view** keyword is not supported.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter `! exclude output`, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

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]]
  [ | {begin | exclude | include} expression]
```

Syntax Description

cpu-queue-map-table [asic number port number [asic number]]	Display the CPU queue-map table entries. The keywords have these meanings: asic number—(Optional) Display information for the specified ASIC. The range is 0 to 1. port number—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.
dest-map index <i>number</i>	Display destination-map information for the specified index. The range is 0 to 65535.
etherchannel-info [asic number port number [asic number]]	Display the contents of the EtherChannel information register. The keywords have these meanings: asic number—(Optional) Display information for the specified ASIC. The range is 0 to 1. port number—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.

exception [<i>asic number</i> port number [<i>asic number</i>]]	Display the exception-index register information. The keywords have these meanings: • asic number—(Optional) Display information for the specified ASIC. The range is 0 to 1. • port number—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.
global-status [<i>asic number</i> port number [<i>asic number</i>]]	Display global and interrupt status. The keywords have these meanings: • asic number—(Optional) Display information for the specified ASIC. The range is 0 to 1. • port number—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.
learning [<i>asic number</i> port number [<i>asic number</i>]]	Display entries in the learning cache. The keywords have these meanings: • asic number—(Optional) Display information for the specified ASIC. The range is 0 to 1. • port number—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.
mac-info [<i>asic number</i> port number [<i>asic number</i>]]	Display the contents of the MAC information register. The keywords have these meanings: • asic number—(Optional) Display information for the specified ASIC. The range is 0 to 1. • port number—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.
mvid [<i>asic number</i>]	Display the mapped VLAN ID table. The keyword has this meaning: • asic number—(Optional) Display information for the specified ASIC. The range is 0 to 1.
packet-info-ram [<i>asic number</i> <i>index number</i> [<i>asic number</i>]]	Display the packet information RAM. The keywords have these meanings: • asic number—(Optional) Display information for the specified ASIC. The range is 0 to 1. • index number—(Optional) Display information for the specified packet RAM index number and ASIC number. The range is 0 to 63.

port-info [<i>asic number</i> port number [<i>asic number</i>]]	Display port information register values. The keywords have these meanings: • asic number—(Optional) Display information for the specified ASIC. The range is 0 to 1. • port number—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.
prog-parser [<i>asic number</i> port number [<i>asic number</i>]]	Display the programmable parser tables. The keywords have these meanings: • asic number—(Optional) Display information for the specified ASIC. The range is 0 to 1. • port number—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.
receive { buffer-queue port-fifo supervisor-sram } [<i>asic number</i> port number [<i>asic number</i>]]	Display receive information. The keywords have these meanings: • buffer-queue—Display the buffer queue information. • port-fifo—Display the port-FIFO information. • supervisor-sram—Display the supervisor static RAM (SRAM) information. • asic number—(Optional) Display information for the specified ASIC. The range is 0 to 1. • port number—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.
span [<i>vlan-id</i> asic number]	Display the Switched Port Analyzer (SPAN)-related information. The keywords have these meanings: • <i>vlan-id</i>—(Optional) Display information for the specified VLAN. The range is 0 to 1023. • asic number—(Optional) Display information for the specified ASIC. The range is 0 to 1.
stats { drop enqueue miscellaneous supervisor } [<i>asic number</i> port number [<i>asic number</i>]]	Display raw statistics for the port ASIC. The keywords have these meanings: • drop—Display drop statistics. • enqueue—Display enqueue statistics. • miscellaneous—Display miscellaneous statistics. • supervisor—Display supervisor statistics. • asic number—(Optional) Display information for the specified ASIC. The range is 0 to 1. • port number—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.

transmit { port-fifo queue supervisor-sram } [asic number port number [asic number]]	Display transmit information. The keywords have these meanings: • port-fifo—Display the contents of the port-FIFO information register. • queue—Display the contents of the queue information register. • supervisor-sram—Display supervisor SRAM information. • asic number—(Optional) Display information for the specified ASIC. The range is 0 to 1. • port number—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.
vct [asic number port number [asic number]]	Display the VLAN compression table entries for the specified ASIC or for the specified port and ASIC. The keywords have these meanings: • asic number—(Optional) Display information for the specified ASIC. The range is 0 to 1. • port number—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

**Note**

Though visible in the command-line help strings, the **stack** { **control** | **dest-map** | **learning** | **messages** | **mvid** | **prog-parser** | **span** | **stats** [**asic number** | **port number** [**asic number**]] keywords are not supported.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

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

show platform port-security

Use the **show platform port-security** privileged EXEC command to display platform-dependent port-security information.

show platform port-security [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.
	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

show platform qos

Use the **show platform qos** privileged EXEC command to display platform-dependent quality of service (QoS) information.

```
show platform qos {label asic number | policer {parameters asic number |
port alloc number asic number}} [ | {begin | exclude | include} expression]
```

Syntax Description	
label asic number	Display QoS label maps for the specified ASIC. (Optional) For asic number , the range is 0 to 1.
policer {parameters asic number port alloc number asic number}	Display policer information. The keywords have these meanings: parameters asic number—Display parameter information for the specified ASIC. The range is 0 to 1. port alloc number asic number—Display port allocation information for the specified port and ASIC. The port allocation range is 0 to 25. The ASIC range is 0 to 1.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so. Expressions are case sensitive. For example, if you enter exclude output, the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

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 | sd [index number] |
vld [index number]} [ | {begin | exclude | include} expression]
```

Syntax Description	
dm [index number]	Display the destination map. The keyword has this meaning: index number—(Optional) Display the specified index. The range is 0 to 65535.
erd [index number]	Display the equal-cost-route descriptor table for the specified index. The keyword has this meaning: index number—(Optional) Display the specified index. The range is 0 to 65535.
mad [index number]	Display the MAC-address descriptor table for the specified index. The keyword has this meaning: index number—(Optional) Display the specified index. The range is 0 to 65535.
med [index number]	Display the multi-expansion descriptor table for the specified index. The keyword has this meaning: index number—(Optional) Display the specified index. The range is 0 to 65535.
mod	Display the resource-manager module information.
sd [index number]	Display the station descriptor table for the specified index. The keyword has this meaning: index number—(Optional) Display the specified index. The range is 0 to 65535.
vld [index number]	Display the VLAN-list descriptor table for the specified index. The keyword has this meaning: index number—(Optional) Display the specified index. The range is 0 to 65535.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter `! exclude output`, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

show platform snmp counters

Use the **show platform snmp counters** privileged EXEC command to display platform-dependent Simple Network Management Protocol (SNMP) counter information.

show platform snmp counters [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.
	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

show platform spanning-tree

Use the **show platform spanning-tree** privileged EXEC command to display platform-dependent spanning-tree information.

show platform spanning-tree synchronization [**detail** | **vlan** *vlan-id*] [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description	synchronization [detail vlan <i>vlan-id</i>]	Display spanning-tree state synchronization information. The keywords have these meanings: • detail—(Optional) Display detailed spanning-tree information. • vlan <i>vlan-id</i>—(Optional) Display VLAN switch spanning-tree information for the specified VLAN. The range is 1 to 4094.
	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so. Expressions are case sensitive. For example, if you enter exclude output, the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

show platform stp-instance

Use the **show platform stp-instance** privileged EXEC command to display platform-dependent spanning-tree instance information.

```
show platform stp-instance vlan-id [ | { begin | exclude | include } expression]
```

Syntax Description	<i>vlan-id</i>	Display spanning-tree instance information for the specified VLAN. The range is 1 to 4094.
	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

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

show platform tb

Use the **show platform tb** privileged EXEC command to display platform-dependent trusted-boundary information during a stack master change to a new stack master.

show platform tb [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines	You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so. Expressions are case sensitive. For example, if you enter exclude output, the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.

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 | ipv6 {acl | qos | secondary} | 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]] [ | {begin | exclude | include} expression]
```

```
show platform tcam table acl [asic number [detail [invalid]] | [index number [detail [invalid]] | invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number [detail [invalid]] | invalid]] [ | {begin | exclude | include} expression]
```

```
show platform tcam table all [asic number [detail [invalid]] | [index number [detail [invalid]] | invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number [detail [invalid]] | invalid]] [ | {begin | exclude | include} expression]
```

```
show platform tcam table equal-cost-route [asic number [detail [invalid]] | [index number [detail [invalid]] | invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number [detail [invalid]] | invalid]] [ | {begin | exclude | include} expression]
```

```
show platform tcam table ipv6 {acl | qos | secondary} [asic number [detail [invalid]] | [index number [detail [invalid]] | invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number [detail [invalid]] | invalid]] [ | {begin | exclude | include} expression]
```

```
show platform tcam table local [asic number [detail [invalid]] | [index number [detail [invalid]] | invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number [detail [invalid]] | invalid]] [ | {begin | exclude | include} expression]
```

```
show platform tcam table mac-address [asic number [detail [invalid]] | [index number [detail [invalid]] | invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number [detail [invalid]] | invalid]] [ | {begin | exclude | include} expression]
```

```
show platform tcam table multicast-expansion [asic number [detail [invalid]] | [index number [detail [invalid]] | invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number [detail [invalid]] | invalid]] [ | {begin | exclude | include} expression]
```

```
show platform tcam table qos [asic number [detail [invalid]] | [index number [detail [invalid]] | invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number [detail [invalid]] | invalid]] [ | {begin | exclude | include} expression]
```

```
show platform tcam table secondary [asic number [detail [invalid]] | [index number [detail [invalid]] | invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number [detail [invalid]] | invalid]] [ | {begin | exclude | include} expression]
```

```
show platform tcam table station [asic number [detail [invalid]] | [index number [detail [invalid]] | invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number [detail [invalid]] | invalid]] [ | {begin | exclude | include} expression]
```

```
show platform tcam table vlan-list [[asic number [detail [invalid]] | [index number [detail [invalid]] | invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number [detail [invalid]] | invalid]] [ | {begin | exclude | include} expression]
```

Syntax Description		
	handle <i>number</i>	Display the TCAM handle. The range is 0 to 4294967295.
	log-results	Display the TCAM log results.
	table { acl all equal-cost-route ipv6 { acl qos secondary } local mac-address multicast-expansion qos secondary station vlan-list }	Display lookup and forwarding table information. The keywords have these meanings: • acl—Display the access-control list (ACL) table. • all—Display all the TCAM tables. • equal-cost-route—Display the equal-cost-route table. • ipv6—Display IPv6 information. – acl—Display the IPv6 ACL-table information. – qos—Display the IPv6 QoS-table information. – secondary—Display the IPv6 secondary-table information. • local—Display the local table. • mac-address—Display the MAC-address table. • multicast-expansion—Display the IPv6 multicast-expansion table. • qos—Display the QoS table. • secondary—Display the secondary table. • station—Display the station table. • vlan-list—Display the VLAN list table.
	usage	Display the CAM and forwarding table usage.
	[[asic <i>number</i> [detail [invalid]] [index <i>number</i> [detail [invalid]] invalid num <i>number</i> [detail [invalid]] [invalid]] [invalid]] [invalid]] [num <i>number</i> [detail [invalid]] [invalid]]	Display information. The keywords have these meanings: • asic <i>number</i>—Display information for the specified ASIC device ID. The range is 0 to 15. • detail [invalid]—(Optional) Display valid or invalid details. • index <i>number</i>—(Optional) Display information for the specified TCAM table index. The range is 0 to 32768. • num <i>number</i>—(Optional) Display information for the specified TCAM table number. The range is 0 to 32768.
	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes Privileged EXEC

 show platform tcam

Command History

Release	Modification
12.1(14)AX	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

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

show platform vlan

Use the **show platform vlan** privileged EXEC command to display platform-dependent VLAN information.

```
show platform vlan { misc | mvid | prune | refcount | rpc { receive | transmit } } [ | { begin | exclude | include } expression]
```

Syntax Description	
misc	Display miscellaneous VLAN module information.
mvid	Display the mapped VLAN ID (MVID) allocation information.
prune	Display the platform-maintained pruning database.
refcount	Display the VLAN lock module-wise reference counts.
rpc { receive transmit }	Display remote procedure call (RPC) messages. The keywords have these meanings: receive—Display received information. transmit—Display transmitted information.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(14)AX	This command was introduced.

Usage Guidelines

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

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

■ show platform vlan



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

Numerics

- 802.1Q tunnel ports
 - and QoS guidelines [2-248, 2-280](#)
 - configuring [2-666](#)
 - displaying [2-416](#)
 - limitations [2-667](#)
- 802.1x
 - and switchport modes [2-667](#)
 - See also port-based authentication
 - violation error recovery [2-108](#)

A

- aaa accounting dot1x command [2-1](#)
- aaa authentication dot1x command [2-3](#)
- AAA methods [2-3](#)
- abort command [2-724](#)
- access control entries
 - See ACEs
- access control lists
 - See ACLs
- access groups
 - IP [2-128](#)
 - MAC, displaying [2-488](#)
- access lists
 - IP [2-128](#)
 - on Layer 2 interfaces [2-128](#)
- access map configuration mode [2-235](#)
- access mode [2-666](#)
- access ports [2-666](#)
- ACEs [2-75, 2-306](#)

ACLs

- deny [2-73](#)
- displaying [2-389](#)
- for non-IP protocols [2-213](#)
- matching [2-235](#)
- permit [2-304](#)
- action command [2-5](#)
- address aliasing [2-293](#)
- aggregate-port learner [2-300](#)
- allowed VLANs [2-684](#)
- Any Transport over MPLS
 - See AToM
- apply command [2-724](#)
- archive download-sw command [2-7](#)
- archive tar command [2-9](#)
- archive upload-sw command [2-12](#)
- arp access-list command [2-13](#)
- AToM, debug messages [B-23](#)
- audience [xix](#)
- authentication failed VLAN
 - See dot1x auth-fail vlan
- auth-fail max-attempts
 - See dot1x auth-fail max-attempts
- auth-fail vlan
 - See dot1x auth-fail vlan
- authorization state of controlled port [2-90](#)
- autonegotiation of duplex mode [2-101](#)
- auto-QoS
 - See QoS
- auto qos voip command [2-15](#)

B

BackboneFast, for STP [2-598](#)

backup interfaces

- configuring [2-657, 2-660](#)
- displaying [2-437](#)

bandwidth command [2-20](#)

boot (boot loader) command [A-2](#)

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

- displaying environment variables [2-398](#)
- interrupting [2-24](#)
- IOS image [2-29](#)
- manually [2-27](#)

boot loader

- accessing [A-1](#)
- booting

 - helper image [2-25](#)
 - IOS image [A-2](#)

directories

- creating [A-15](#)
- displaying a list of [A-7](#)
- removing [A-19](#)

displaying

- available commands [A-12](#)
- memory heap utilization [A-13](#)
- version [A-26](#)

environment variables

- described [A-20](#)
- displaying settings [A-20](#)
- location of [A-21](#)
- setting [A-20](#)
- unsetting [A-24](#)

boot loader (continued)

files

- copying [A-5](#)
- deleting [A-6](#)
- displaying a list of [A-7](#)
- displaying the contents of [A-4, A-16, A-23](#)
- renaming [A-17](#)

file system

- formatting [A-10](#)
- initializing flash [A-9](#)
- running a consistency check [A-11](#)

prompt [A-1](#)

resetting the system [A-18](#)

boot manual command [2-27](#)

boot private-config-file command [2-28](#)

boot system command [2-29](#)

BPDU filtering, for spanning tree [2-599, 2-633](#)

BPDU guard, for spanning tree [2-601, 2-633](#)

broadcast storm control [2-650](#)

bundling characteristics, UNI [2-113](#)

C

candidate switches

- See clusters

cat (boot loader) command [A-4](#)

caution, description [xx](#)

CDP, enabling protocol tunneling for [2-192](#)

CFM [2-299](#)

CFM as OAM protocol [2-299](#)

channel-group command [2-30](#)

channel-protocol command [2-34](#)

Cisco SoftPhone, auto-QoS configuration [2-15](#)

class command [2-35](#)

class-map command [2-39](#)

class maps

- creating [2-39](#)
- defining the match criteria [2-237](#)
- displaying [2-400](#)

class of service

See CoS

clear ip arp inspection log command [2-41](#)

clear ip arp inspection statistics command [2-42](#)

clear l2protocol-tunnel counters command [2-45](#)

clear lacp command [2-46](#)

clear mac address-table command [2-47, 2-48](#)

clear pagp command [2-49, 2-50](#)

clear spanning-tree counters command [2-51](#)

clear spanning-tree detected-protocols command [2-52](#)

clear vmps statistics command [2-53](#)

clear vtp counters command [2-54](#)

cluster commander-address command [2-55](#)

cluster discovery hop-count command [2-57](#)

cluster enable command [2-58](#)

cluster holdtime command [2-60](#)

cluster member command [2-61](#)

cluster outside-interface command [2-63](#)

cluster run command [2-64](#)

clusters

adding candidates [2-61](#)

binding to HSRP group [2-65](#)

building manually [2-61](#)

communicating with

devices outside the cluster [2-63](#)

members by using Telnet [2-350](#)

debug messages, display [B-5](#)

displaying

candidate switches [2-403](#)

debug messages [B-5](#)

member switches [2-405](#)

status [2-401](#)

hop-count limit for extended discovery [2-57](#)

HSRP standby groups [2-65](#)

redundancy [2-65](#)

SNMP trap [2-588](#)

cluster standby-group command [2-65](#)

cluster timer command [2-67](#)

command modes defined [1-1](#)

command switch

See clusters

configuration, initial

See hardware installation guide

configuration files

password recovery disable considerations [A-1](#)

specifying the name [2-23, 2-28](#)

configuring multiple interfaces [2-124](#)

config-vlan mode

commands [2-710](#)

description [1-4](#)

entering [2-709](#)

summary [1-2](#)

conventions

command [xix](#)

for examples [xx](#)

publication [xix](#)

text [xix](#)

copy (boot loader) command [A-5](#)

CoS

assigning default value to incoming packets [2-246](#)

assigning to Layer 2 protocol packets [2-196](#)

overriding the incoming value [2-246](#)

CoS-to-DSCP map [2-252](#)

CPU ASIC statistics, displaying [2-407](#)

cpu traffic qos [2-68](#)

D

debug autoqos command [B-2](#)

debug backup command [B-4](#)

debug cluster command [B-5](#)

debug dot1x command [B-7](#)

debug dtp command [B-8](#)

debug etherchannel command [B-9](#)

debug interface command [B-12](#)

debug ip dhcp snooping command [B-13](#)

debug ip igmp filter command [B-14](#)

debug ip igmp max-groups command [B-15](#)

- debug ip igmp snooping command [B-16](#)
- debug ip verify source packet command [B-17](#)
- debug lacp command [B-18](#)
- debug mac-notification command [B-19](#)
- debug matm command [B-20](#)
- debug matm move update command [B-21](#)
- debug monitor command [B-22](#)
- debug mpls atom command [B-23](#)
- debug mpls l2transport vlan command [B-24](#)
- debug mvrdbg command [B-25](#)
- debug nvram command [B-26](#)
- debug pagp command [B-27](#)
- debug platform acl command [B-28](#)
- debug platform backup interface command [B-30](#)
- debug platform cfm command [B-29](#)
- debug platform cpu-queues command [B-31](#)
- debug platform dot1x command [B-33](#)
- debug platform etherchannel command [B-34](#)
- debug platform fallback-bridging command [B-35](#)
- debug platform forw-tcam command [B-36](#)
- debug platform ip arp inspection command [B-37](#)
- debug platform ip igmp snooping command [B-38](#)
- debug platform ip multicast command [B-40](#)
- debug platform ip unicast command [B-42](#)
- debug platform led command [B-44](#)
- debug platform matm command [B-45](#)
- debug platform messaging command [B-46](#)
- debug platform mpls command [B-47](#)
- debug platform phy command [B-48](#)
- debug platform pm command [B-49](#)
- debug platform port-asic command [B-51](#)
- debug platform port-security command [B-52](#)
- debug platform qos-acl-tcam command [B-53](#)
- debug platform remote-commands command [B-54](#)
- debug platform rep command [B-55](#)
- debug platform resource-manager command [B-56](#)
- debug platform snmp command [B-57](#)
- debug platform span command [B-58](#)
- debug platform supervisor-asic command [B-59](#)
- debug platform sw-bridge command [B-60](#)
- debug platform tcam command [B-61](#)
- debug platform udd command [B-63](#)
- debug platform vlan command [B-64](#)
- debug pm command [B-65](#)
- debug port-security command [B-67](#)
- debug qos-manager command [B-69](#)
- debug rep command [B-68](#)
- debug spanning-tree backbonefast command [B-72](#)
- debug spanning-tree bpdu command [B-73](#)
- debug spanning-tree bpdu-opt command [B-74](#)
- debug spanning-tree command [B-70](#)
- debug spanning-tree mstp command [B-75](#)
- debug spanning-tree switch command [B-77](#)
- debug spanning-tree uplinkfast command [B-79](#)
- debug sw-vlan command [B-80](#)
- debug sw-vlan ifs command [B-82](#)
- debug sw-vlan notification command [B-83](#)
- debug sw-vlan vtp command [B-84](#)
- debug udd command [B-86](#)
- debug vqpc command [B-88](#)
- debug xconnect command [B-89](#)
- default template [2-370](#)
- define interface-range command [2-70](#)
- delete (boot loader) command [A-6](#)
- delete command [2-72](#)
- deny (ARP access-list configuration) command [2-76](#)
- deny command [2-73](#)
- detect mechanism, causes [2-103](#)
- DHCP snooping
 - accepting untrusted packets from edge switch [2-153](#)
 - enabling
 - on a VLAN [2-159](#)
 - option 82 [2-151, 2-153](#)
 - trust on an interface [2-157](#)
 - rate limiting [2-156](#)

- DHCP snooping binding database
 - binding file, configuring [2-149](#)
 - bindings
 - adding [2-147](#)
 - deleting [2-147](#)
 - clearing database agent statistics [2-43](#)
 - database agent, configuring [2-149](#)
 - displaying
 - database agent status [2-461, 2-463](#)
 - renewing [2-354](#)
- Digital Optical Monitoring
 - see DoM
- dir (boot loader) command [A-7](#)
- directories, deleting [2-72](#)
- documentation, related [xx](#)
- document conventions [xix](#)
- DoM
 - displaying supported transceivers [2-450](#)
- domain name, VTP [2-733, 2-737](#)
- domains, CFM [2-299](#)
- dot1x auth-fail max-attempts [2-78](#)
- dot1x auth-fail vlan [2-80](#)
- dot1x default command [2-82](#)
- dot1x guest-vlan command [2-83](#)
- dot1x host-mode command [2-85](#)
- dot1x initialize command [2-87](#)
- dot1x max-req command [2-88, 2-89](#)
- dot1x port-control command [2-90](#)
- dot1x re-authenticate command [2-92](#)
- dot1x reauthentication command [2-93](#)
- dot1x system-auth-control command [2-94](#)
- dot1x test eapol-capable command [2-95](#)
- dot1x test timeout command [2-96](#)
- dot1x timeout command [2-97](#)
- dot1x violation-mode command [2-99](#)
- dropping packets, with ACL matches [2-5](#)
- drop threshold, Layer 2 protocol tunneling [2-192](#)
- DSCP-to-CoS map [2-252](#)
- DSCP-to-DSCP-mutation map [2-252](#)
- DTP [2-667](#)
- DTP flap
 - error detection for [2-103](#)
 - error recovery timer [2-108](#)
- dual-level policy maps [2-321](#)
- duplex command [2-101](#)
- dynamic-access ports
 - configuring [2-655](#)
 - restrictions [2-655](#)
- dynamic ARP inspection
 - ARP ACLs
 - apply to a VLAN [2-133](#)
 - define [2-13](#)
 - deny packets [2-76](#)
 - display [2-393](#)
 - permit packets [2-307](#)
 - clear
 - log buffer [2-41](#)
 - statistics [2-42](#)
 - display
 - ARP ACLs [2-393](#)
 - configuration and operating state [2-454](#)
 - log buffer [2-454](#)
 - statistics [2-454](#)
 - trust state and rate limit [2-454](#)
 - enable per VLAN [2-143](#)
 - error detection for [2-108](#)
 - log buffer
 - clear [2-41](#)
 - configure [2-137](#)
 - display [2-454](#)
 - rate-limit incoming ARP packets [2-135](#)
 - statistics
 - clear [2-42](#)
 - display [2-454](#)
 - trusted interface state [2-139](#)
 - type of packet logged [2-144](#)
 - validation checks [2-141](#)
- dynamic auto VLAN membership mode [2-666](#)

dynamic desirable VLAN membership mode [2-666](#)

Dynamic Host Configuration Protocol (DHCP)

See DHCP snooping

Dynamic Trunking Protocol

See DTP

E

EAP-request/identity frame

maximum number to send [2-89](#)

response time before retransmitting [2-97](#)

E-LMI

enabling [2-111](#)

mapping [2-113](#)

encapsulation methods [2-684](#)

environment variables, displaying [2-398](#)

EoMPLS

configuring [2-287, 2-741](#)

displaying [2-528](#)

errdisable detect cause command [2-103](#)

errdisable detect cause small-frame command [2-105](#)

errdisable recovery cause small-frame [2-107](#)

errdisable recovery command [2-108](#)

error conditions, displaying [2-425](#)

error disable detection [2-103](#)

error-disabled interfaces, displaying [2-437](#)

EtherChannel

assigning Ethernet interface to channel group [2-30](#)

creating port-channel logical interface [2-122](#)

debug EtherChannel/PAgP, display [B-9](#)

debug platform-specific events, display [B-34](#)

displaying [2-429](#)

enabling Layer 2 protocol tunneling for

LACP [2-193](#)

PAgP [2-193](#)

UDLD [2-193](#)

interface information, displaying [2-437](#)

LACP

clearing channel-group information [2-46](#)

debug messages, display [B-18](#)

displaying [2-480](#)

modes [2-30](#)

port priority for hot-standby ports [2-197](#)

restricting a protocol [2-34](#)

system priority [2-199](#)

load-distribution methods [2-323](#)

PAgP

aggregate-port learner [2-300](#)

clearing channel-group information [2-49](#)

debug messages, display [B-27](#)

displaying [2-538](#)

error detection for [2-103](#)

error recovery timer [2-108](#)

learn method [2-300](#)

modes [2-30](#)

physical-port learner [2-300](#)

priority of interface for transmitted traffic [2-302](#)

ethermnet lmi ce command [2-111](#)

Ethernet controller, internal register display [2-409](#)

ethernet evc command [2-110](#)

ethernet lim global command [2-111](#)

ethernet lmi ce-vlan map command [2-113, 2-115](#)

ethernet lmi command [2-111](#)

Ethernet Local Management Interface

See E-LMI

Ethernet over MPLS

See EoMPLS

Ethernet over multiprotocol label switching

See EoMPLS

Ethernet service

debugging [B-10](#)

displaying [2-432](#)

Ethernet service instance [2-372](#)

Ethernet service interfaces [2-435](#)

Ethernet statistics, collecting [2-369](#)

Ethernet UNI configuration [2-117](#)

ethernet uni id command [2-119](#)

Ethernet virtual connections

See EVCs

EVC configuration mode [2-110](#)

EVCs [2-110](#)

and VLANs [2-117](#)

service instances [2-372](#)

UNI counts [2-707](#)

EVC service

point-to-multipoint [2-707](#)

point-to-point [2-707](#)

examples, conventions for [xx](#)

exit command, VLAN database mode [2-724](#)

extended discovery of candidate switches [2-57](#)

extended-range VLANs

and allowed VLAN list [2-685](#)

and pruning-eligible list [2-685](#)

configuring [2-709](#)

extended system ID for STP [2-607](#)

F

fan information, displaying [2-422](#)

file name, VTP [2-733](#)

files, deleting [2-72](#)

flash_init (boot loader) command [A-9](#)

Flex Links

configuring [2-657, 2-660](#)

configuring preferred VLAN [2-659, 2-663](#)

displaying [2-437](#)

flowcontrol command [2-120](#)

format (boot loader) command [A-10](#)

forwarding packets, with ACL matches [2-5](#)

forwarding results, display [C-6](#)

frame forwarding information, displaying [C-6](#)

fsck (boot loader) command [A-11](#)

G

global configuration mode [1-2, 1-3](#)

H

hardware ACL statistics [2-389](#)

help (boot loader) command [A-12](#)

hop-count limit for clusters [2-57](#)

host connection, port configuration [2-665](#)

host ports, private VLANs [2-669](#)

HSRP

binding HSRP group to cluster [2-65](#)

standby group [2-65](#)

I

IEEE 802.1ag Connectivity Fault Management

See CFM

IEEE 802.1X Port Based Authentication

enabling guest VLAN supplicant [2-79](#)

IGMP filters

applying [2-162](#)

debug messages, display [B-14](#)

IGMP groups, setting maximum [2-164](#)

IGMP maximum groups, debugging [B-15](#)

IGMP profiles

creating [2-166](#)

displaying [2-466](#)

IGMP snooping

adding ports as a static member of a group [2-177](#)

displaying [2-467, 2-471, 2-473](#)

enabling the Immediate-Leave feature [2-174](#)

multicast table [2-469](#)

querier [2-170](#)

report suppression [2-172](#)

images

See software images

Immediate-Leave feature, MVR [2-295](#)

- immediate-leave processing [2-174](#)
- import map command [2-189](#)
- initial configuration
 - See hardware installation guide
- interface configuration mode [1-2, 1-3](#)
- interface port-channel command [2-122](#)
- interface range command [2-124](#)
- interface-range macros [2-68, 2-70](#)
- interfaces
 - assigning Ethernet interface to channel group [2-30](#)
 - configuring [2-101](#)
 - configuring multiple [2-124](#)
 - creating port-channel logical [2-122](#)
 - debug messages, display [B-12](#)
 - disabling [2-583](#)
 - displaying the MAC address table [2-500](#)
 - restarting [2-583](#)
- interface speed, configuring [2-642](#)
- interface vlan command [2-126](#)
- internal registers, displaying [2-409, 2-413, 2-415](#)
- Internet Group Management Protocol
 - See IGMP
- invalid GBIC
 - error detection for [2-103](#)
 - error recovery timer [2-108](#)
- ip access-group command [2-128](#)
- ip address command [2-131](#)
- IP addresses, setting [2-131](#)
- IP address matching [2-235](#)
- ip arp inspection filter vlan command [2-133](#)
- ip arp inspection limit command [2-135](#)
- ip arp inspection log-buffer command [2-137](#)
- ip arp inspection trust command [2-139](#)
- ip arp inspection validate command [2-141](#)
- ip arp inspection vlan command [2-143](#)
- ip arp inspection vlan logging command [2-144](#)
- IP DHCP snooping
 - See DHCP snooping
- ip dhcp snooping binding command [2-147](#)
- ip dhcp snooping command [2-146](#)
- ip dhcp snooping database command [2-149](#)
- ip dhcp snooping information option allow-untrusted command [2-153](#)
- ip dhcp snooping information option command [2-151](#)
- ip dhcp snooping information option format remote-id command [2-155](#)
- ip dhcp snooping limit rate command [2-156](#)
- ip dhcp snooping trust command [2-157](#)
- ip dhcp snooping verify command [2-158](#)
- ip dhcp snooping vlan command [2-159](#)
- ip dhcp snooping vlan information option format-type circuit-id string command [2-160](#)
- ip igmp filter command [2-162](#)
- ip igmp max-groups command [2-164, 2-183, 2-185](#)
- ip igmp profile command [2-166](#)
- ip igmp snooping command [2-168](#)
- ip igmp snooping querier command [2-170](#)
- ip igmp snooping report-suppression command [2-172](#)
- ip igmp snooping vlan immediate-leave command [2-174](#)
- ip igmp snooping vlan mrouter command [2-175](#)
- ip igmp snooping vlan static command [2-177](#)
- IP multicast addresses [2-292](#)
- IP phones
 - auto-QoS configuration [2-15](#)
 - trusting packets sent from [2-279](#)
- IP-precedence-to-DSCP map [2-252](#)
- ip source binding command [2-179](#)
- IP source guard
 - disabling [2-187](#)
 - displaying
 - binding entries [2-475](#)
 - configuration [2-476](#)
 - enabling [2-187](#)
 - static IP source bindings [2-179](#)
- ip ssh command [2-181](#)
- ip verify source command [2-187](#)
- ip vrf (global configuration) command [2-188](#)
- ip vrf (interface configuration) command [2-190](#)

J

jumbo frames

See MTU

L

l2protocol-tunnel command [2-192](#)

l2protocol-tunnel cos command [2-196](#)

label distribution protocol

See LDP

LACP

See EtherChannel

lacp port-priority command [2-197](#)

lacp system-priority command [2-199](#)

Layer 2 mode, enabling [2-653](#)

Layer 2 protocol ports, displaying [2-478](#)

Layer 2 protocol tunnel

and EtherChannels [2-193](#)

CoS [2-196](#)

counters, clearing [2-45](#)

error detection for [2-103](#)

error recovery [2-194](#)

error recovery timer [2-108](#)

setting thresholds for [2-194](#)

Layer 2 traceroute

IP addresses [2-698](#)

MAC addresses [2-695](#)

Layer 3 mode, enabling [2-653](#)

LDP

destination [2-287](#)

holdtime [2-289](#)

line configuration mode [1-2, 1-5](#)

Link Aggregation Control Protocol

See EtherChannel

link flap

error detection for [2-103](#)

error recovery timer [2-108](#)

link state group command [2-201](#)

link state track command [2-203](#)

load-distribution methods for EtherChannel [2-323](#)

location (global configuration) command [2-204](#)

location (interface configuration) command [2-206](#)

logging event command [2-208](#)

logging file command [2-209](#)

logical interface [2-122](#)

loopback error

detection for [2-103](#)

recovery timer [2-108](#)

loop guard, for spanning tree [2-608, 2-612](#)

M

mac access-group command [2-211](#)

MAC access-groups, displaying [2-488](#)

MAC access list configuration mode [2-213](#)

mac access-list extended command [2-213](#)

MAC access lists [2-73](#)

MAC addresses

disabling MAC address learning per VLAN [2-216](#)

displaying

aging time [2-494](#)

all [2-492](#)

dynamic [2-498](#)

Layer 2 multicast entries [2-505](#)

MAC address-table move updates [2-503](#)

notification settings [2-502, 2-507](#)

number of addresses in a VLAN [2-496](#)

per interface [2-500](#)

per VLAN [2-511](#)

static [2-509](#)

static and dynamic entries [2-490](#)

dynamic

aging time [2-215](#)

deleting [2-47](#)

displaying [2-498](#)

enabling MAC address notification [2-220](#)

enabling MAC address-table move update [2-218](#)

MAC addresses (continued)

- matching [2-235](#)

- static

- adding and removing [2-222](#)

- displaying [2-509](#)

- dropping on an interface [2-223](#)

- tables [2-492](#)

MAC address notification, debugging [B-19](#)mac address-table aging-time [2-211, 2-235](#)mac address-table aging-time command [2-215](#)mac address-table learning command [2-216](#)mac address-table move update [2-218](#)mac address-table move update command [2-218](#)mac address-table notification command [2-220](#)mac address-table static command [2-222](#)mac address-table static drop command [2-223](#)macro description command [2-228](#)macro global command [2-229](#)macro global description command [2-232](#)macro name command [2-233](#)

macros

- adding a description [2-228](#)

- adding a global description [2-232](#)

- applying [2-229](#)

- creating [2-233](#)

- displaying [2-540](#)

- specifying parameter values [2-229](#)

- tracing [2-229](#)

macros, interface range [2-70, 2-124](#)maintenance end points [2-707](#)

manual

- audience [xix](#)

- purpose of [xix](#)

maps

QoS

- defining [2-252](#)

- displaying [2-520](#)

VLAN

- creating [2-721](#)

- defining [2-235](#)

- displaying [2-573](#)

match (access-map configuration) command [2-235](#)match (class-map configuration) command [2-237](#)

maximum transmission unit

- See MTU

mdix auto command [2-240](#)

member switches

- See clusters

memory (boot loader) command [A-13](#)mkdir (boot loader) command [A-15](#)mls qos aggregate-policer command [2-244](#)mls qos command [2-242](#)mls qos cos command [2-246](#)mls qos dscp-mutation command [2-248](#)mls qos enhanced command [2-250](#)mls qos map command [2-252](#)mls qos queue-set output buffers command [2-255](#)mls qos queue-set output threshold command [2-257](#)mls qos srr-queue input bandwidth command [2-261](#)mls qos srr-queue input buffers command [2-263](#)mls qos-srr-queue input cos-map command [2-265](#)mls qos srr-queue input dscp-map command [2-267](#)mls qos srr-queue input priority-queue command [2-269](#)mls qos srr-queue input threshold command [2-271](#)mls qos-srr-queue output cos-map command [2-273](#)mls qos srr-queue output dscp-map command [2-275, 2-277](#)mls qos trust command [2-279](#)mls qos vlan-based command [2-282](#)mode, MVR [2-292](#)Mode button, and password recovery [2-373](#)modes, commands [1-1](#)monitor session command [2-283](#)

more (boot loader) command [A-16](#)

MPLS

MTU [2-290](#)

VCs [2-287, 2-741](#)

mpls l2transport route command [2-287, 2-528](#)

mpls ldp holdtime command [2-289](#)

mpls mtu command [2-290](#)

MSTP

displaying [2-555](#)

interoperability [2-52](#)

link type [2-610](#)

MST region

aborting changes [2-616](#)

applying changes [2-616](#)

configuration name [2-616](#)

configuration revision number [2-616](#)

current or pending display [2-616](#)

displaying [2-555](#)

MST configuration mode [2-616](#)

VLANs-to-instance mapping [2-616](#)

path cost [2-618](#)

protocol mode [2-614](#)

restart protocol migration process [2-52](#)

root port

loop guard [2-608](#)

preventing from becoming designated [2-608](#)

restricting which can be root [2-608](#)

root guard [2-608](#)

root switch

affects of extended system ID [2-607](#)

hello-time [2-621, 2-629](#)

interval between BPDU messages [2-622](#)

interval between hello BPDU messages [2-621, 2-629](#)

max-age [2-622](#)

maximum hop count before discarding BPDU [2-623](#)

port priority for selection of [2-626](#)

primary or secondary [2-629](#)

MSTP (continued)

switch priority [2-628](#)

state changes

blocking to forwarding state [2-635](#)

enabling BPDU filtering [2-599, 2-633](#)

enabling BPDU guard [2-601, 2-633](#)

enabling Port Fast [2-633, 2-635](#)

forward-delay time [2-620](#)

length of listening and learning states [2-620](#)

rapid transition to forwarding [2-610](#)

shutting down Port Fast-enabled ports [2-633](#)

state information display [2-554](#)

MTU

configuring size [2-693](#)

displaying global setting [2-562](#)

for MPLS [2-290](#)

multicast group address, MVR [2-295](#)

multicast groups, MVR [2-293](#)

multicast router learning method [2-175](#)

multicast router ports, configuring [2-175](#)

multicast storm control [2-650](#)

multicast VLAN, MVR [2-292](#)

multicast VLAN registration

See MVR

multiple hosts on authorized port [2-85](#)

Multiple Spanning Tree Protocol

See MSTP

multiplexing, UNI [2-117](#)

multi VPN routing/forwarding instances in customer edge devices

See multi-VRF CE

multi-VRF CE [2-188, 2-190](#)

MVR

and address aliasing [2-293](#)

configuring [2-292](#)

configuring interfaces [2-295](#)

debug messages, display [B-25](#)

displaying [2-532](#)

MVR (continued)

- displaying interface information [2-534](#)
- members, displaying [2-536](#)
- mvr (global configuration) command [2-292](#)
- mvr (interface configuration) command [2-295](#)
- mvr vlan group command [2-296](#)

N

- native VLANs [2-684](#)
- nonegotiate, DTP messaging [2-671](#)
- nonhierarchical single-level policy maps [2-321](#)
- non-IP protocols
 - denying [2-73](#)
 - forwarding [2-304](#)
- non-IP traffic
 - access lists [2-213](#)
 - denying [2-73](#)
 - permitting [2-304](#)
- normal-range VLANs [2-709, 2-715](#)
- note, description [xx](#)
- no vlan command [2-709, 2-719](#)

O

- OAM PDUs [2-115](#)
- OAM protocol [2-299](#)
- oam protocol cfm svlan command [2-299](#)
- operation, administration, and maintenance protocol
 - See OAM

P

PAgP

See EtherChannel

- pagp learn-method command [2-300](#)
- pagp port-priority command [2-302](#)
- password, VTP [2-733, 2-737](#)

password-recovery mechanism, enabling and disabling [2-373](#)

permit (ARP access-list configuration) command [2-307](#)

permit command [2-304](#)

per-VLAN spanning-tree plus

See STP

physical-port learner [2-300](#)

PID, displaying [2-453](#)

PIM-DVMRP, as multicast router learning method [2-175](#)

police aggregate command [2-311](#)

police cir command [2-313](#)

police cir percent command [2-316](#)

police command [2-309](#)

policed-DSCP map [2-252](#)

policers

aggregate [2-244, 2-311](#)

displaying [2-514](#)

policed-DSCP map [2-252](#)

single-rate ingress [2-309](#)

two-rate hierarchical [2-313, 2-316](#)

policy-map command [2-320](#)

policy maps

applying to an interface [2-375](#)

creating [2-320](#)

displaying [2-543](#)

dual-level [2-321](#)

marking [2-380](#)

nonhierarchical and single-level [2-321](#)

See also policers

See also QoS, hierarchical policies

traffic classification

defining the class [2-35](#)

defining trust states [2-700](#)

Port Aggregation Protocol

See EtherChannel

port-based authentication

- 802.1x AAA accounting methods [2-1](#)
- AAA method list [2-3](#)
- configuring violation modes [2-99](#)
- debug messages, display [B-7](#)
- enabling 802.1x
 - globally [2-94](#)
 - per interface [2-90](#)
- guest VLAN [2-83](#)
- host modes [2-85](#)
- initialize an interface [2-87, 2-96](#)
- manual control of authorization state [2-90](#)
- multiple hosts on authorized port [2-85](#)
- periodic re-authentication
 - enabling [2-93](#)
 - time between attempts [2-97](#)
- quiet period between failed authentication exchanges [2-97](#)
- re-authenticating 802.1x-enabled ports [2-92](#)
- resetting configurable 802.1x parameters [2-82](#)
- statistics and status display [2-417](#)
- switch-to-authentication server retransmission time [2-97](#)
- switch-to-client frame-retransmission number [2-88, 2-89](#)
- switch-to-client retransmission time [2-97](#)
- test for IEEE 802.1x readiness [2-95](#)

port-channel load-balance command [2-323](#)Port Fast, for spanning tree [2-635](#)port ranges, defining [2-68, 2-70](#)ports, debugging [B-65](#)ports, protected [2-683](#)

port security

- aging [2-677](#)
- debug messages, display [B-67](#)
- enabling [2-673](#)
- violation error recovery [2-108](#)

port trust states for QoS [2-279](#)port types, MVR [2-295](#)power information, displaying [2-422](#)priority command [2-325](#)priority-queue command [2-327](#)private-vlan command [2-329](#)private-vlan mapping command [2-332](#)

private VLANs

- association [2-681](#)
- configuring [2-329](#)
- configuring ports [2-669](#)
- displaying [2-568](#)
- host ports [2-669](#)
- mapping
 - configuring [2-681](#)
 - promiscuous ports [2-669](#)

privileged EXEC mode [1-2, 1-3](#)product identification information, displaying [2-453](#)promiscuous ports, private VLANs [2-669](#)protected ports, displaying [2-442](#)

pruning

- VLANs [2-684](#)
- VTP
 - displaying interface information [2-437](#)
 - enabling [2-733, 2-737](#)

pruning-eligible VLAN list [2-686](#)

PVST+

See STP

Q

QoS

- and 802.1Q tunneling guidelines [2-238, 2-248, 2-280](#)
- applying bandwidth to only one ES port [2-250](#)
- auto-QoS
 - configuring [2-15](#)
 - debug messages, display [1-5, B-2](#)
 - displaying [2-394](#)
- class maps
 - creating [2-39](#)
 - defining the match criteria [2-237](#)
 - displaying [2-400](#)

QoS (continued)

defining the CoS value for an incoming packet [2-246](#)

displaying configuration information [2-394, 2-513](#)

DSCP trusted ports

applying DSCP-to-DSCP-mutation map to [2-248](#)

defining DSCP-to-DSCP-mutation map [2-252](#)

egress queues

displaying queue-set settings [2-525](#)

egress queue-sets

allocating buffers [2-255](#)

defining the CoS output queue threshold map [2-273](#)

defining the DSCP output queue threshold map [2-277](#)

displaying buffer allocations [2-517](#)

displaying CoS output queue threshold map [2-520](#)

displaying DSCP output queue threshold map [2-520](#)

displaying queueing strategy [2-517](#)

displaying queue-set settings [2-523](#)

enabling bandwidth shaping and scheduling [2-646](#)

enabling bandwidth sharing and scheduling [2-648](#)

enabling the priority queue [2-327](#)

limiting the maximum output on a port [2-644](#)

mapping a port to a queue-set [2-336](#)

mapping CoS values to a queue and threshold [2-273](#)

mapping DSCP values to a queue and threshold [2-277](#)

setting maximum and reserved memory allocations [2-257](#)

setting WTD thresholds [2-257](#)

SRR and priority queue interaction [2-327](#)

enabling [2-242](#)

QoS (continued)

hierarchical policies

applying to an interface [2-375](#)

average-rate traffic shaping on a class [2-387](#)

bandwidth allocation for a class [2-20](#)

class-based weighted fair queueing [2-20, 2-36](#)

creating a service policy [2-378](#)

displaying [2-543](#)

DSCP-based WRED [2-340](#)

IP precedence-based WRED [2-347](#)

marking [2-380](#)

strict priority queueing (LLQ) [2-325](#)

tail drop [2-334](#)

two-rate policers [2-313, 2-316](#)

WRED [2-337](#)

WRED average queue size calculation [2-344](#)

ingress queues

allocating buffers [2-263](#)

assigning SRR scheduling weights [2-261](#)

defining the CoS input queue threshold map [2-265](#)

defining the DSCP input queue threshold map [2-267](#)

displaying buffer allocations [2-517](#)

displaying CoS input queue threshold map [2-520](#)

displaying DSCP input queue threshold map [2-520](#)

displaying queueing strategy [2-517](#)

displaying settings for [2-515](#)

enabling the priority queue [2-269](#)

mapping CoS values to a queue and threshold [2-265](#)

mapping DSCP values to a queue and threshold [2-267](#)

setting WTD thresholds [2-271](#)

maps

defining [2-252, 2-265, 2-267, 2-273, 2-277](#)

displaying [2-520](#)

QoS (continued)

policy maps

- applying an aggregate policer [2-311](#)
- applying to an interface [2-375](#)
- creating [2-320](#)
- defining aggregate policers [2-244](#)
- defining single-rate ingress policers [2-309](#)
- displaying policers [2-514](#)
- displaying policy maps [2-543](#)
- dual-level [2-321](#)
- hierarchical on non-ES ports [2-321](#)
- marking [2-380](#)
- policed-DSCP map [2-252](#)
- traffic classifications [2-35](#)
- trust states [2-700](#)

port trust states [2-279](#)

statistics

- in-profile and out-of-profile packets [2-517](#)
- packets enqueued or dropped [2-517](#)
- sent and received CoS values [2-517](#)
- sent and received DSCP values [2-517](#)

trusted boundary for IP phones [2-279](#)VLAN-based [2-282](#)

quality of service

See QoS

querytime, MVR [2-292](#)queue-limit command [2-334](#)queue-set command [2-336](#)**R**random-detect command [2-337](#)random-detect dscp command [2-340](#)random-detect exponential-weighting-constant command [2-344](#)random-detect precedence command [2-347](#)

rapid per-VLAN spanning-tree plus

See STP

rapid PVST+

See STP

rcommand command [2-350](#)re-authenticating 802.1x-enabled ports [2-92](#)

re-authentication

- periodic [2-93](#)
- time between attempts [2-97](#)

receiver ports, MVR [2-295](#)receiving flow-control packets [2-120](#)

recovery mechanism

- causes [2-108](#)
- display [2-423, 2-427](#)
- timer interval [2-108](#)

redundancy for cluster switches [2-65](#)remote-span command [2-352](#)

Remote Switched Port Analyzer

See RSPAN

rename (boot loader) command [A-17](#)renew ip dhcp snooping database command [2-354](#)rep admin vlan command [2-355](#)rep block port command [2-356](#)rep lsl-age-timer command [2-359](#)rep preempt delay command [2-360](#)rep preempt segment command [2-362](#)rep segment command [2-363](#)rep stcn command [2-366](#)reset (boot loader) command [A-18](#)reset command [2-724](#)resource templates, displaying [2-551](#)

restricted VLAN

See dot1x auth-fail vlan

rmdir (boot loader) command [A-19](#)rmon collection stats command [2-369](#)root guard, for spanning tree [2-608](#)route distinguisher [2-189](#)

routed ports

- IP addresses on [2-132](#)
- number supported [2-132](#)

route-target command [2-189](#)

routing template [2-370](#)

RSPAN

configuring [2-283](#)

displaying [2-526](#)

filter RSPAN traffic [2-283](#)

sessions

add interfaces to [2-283](#)

displaying [2-526](#)

start new [2-283](#)

VLAN [2-352](#)

S

sdm prefer command [2-370](#)

secure ports, limitations [2-674](#)

sending flow-control packets [2-120](#)

service instance command [2-372](#)

service instances, displaying [2-433](#)

service password-recovery command [2-373](#)

service-policy command (interface configuration) [2-375](#)

service-policy command (policy-map class) [2-378](#)

set (boot loader) command [A-20](#)

set command [2-380](#)

setup command [2-382](#)

setup express command [2-385](#)

shape command [2-387](#)

show access-lists command [2-389](#)

show archive status command [2-392](#)

show arp access-list command [2-393](#)

show auto qos command [2-394](#)

show boot command [2-398](#)

show changes command [2-724](#)

show class-map command [2-400](#)

show cluster candidates command [2-403](#)

show cluster command [2-401](#)

show cluster members command [2-405](#)

show controllers cpu-interface command [2-407](#)

show controllers ethernet-controller command [2-409](#)

show controllers team command [2-413](#)

show cpu traffic qos [2-415](#)

show current command [2-724](#)

show dot1q-tunnel command [2-416](#)

show dot1x command [2-417](#)

show dtp command [2-420](#)

show env command [2-422](#)

show errdisable detect command [2-423](#)

show errdisable flap-values command [2-425](#)

show errdisable recovery command [2-427](#)

show etherchannel command [2-429](#)

show ethernet service evc command [2-432](#)

show ethernet service instance command [2-433](#)

show ethernet service interface command [2-435](#)

show interface rep command [2-448](#)

show interfaces command [2-437](#)

show interfaces counters command [2-445](#)

show interface transceivers command [2-450](#)

show inventory command [2-453](#)

show ip arp inspection command [2-454](#)

show ip dhcp snooping binding command [2-459](#)

show ip dhcp snooping command [2-458](#)

show ip dhcp snooping database command [2-461, 2-463](#)

show ip igmp profile command [2-466](#)

show ip igmp snooping command [2-467](#)

show ip igmp snooping groups command [2-469](#)

show ip igmp snooping mrouter command [2-471](#)

show ip igmp snooping querier command [2-473](#)

show ip source binding command [2-475](#)

show ip verify source command [2-476](#)

show l2protocol-tunnel command [2-478](#)

show lacp command [2-480](#)

show link state group command [2-484](#)

show location [2-486](#)

show location command [2-486](#)

show mac access-group command [2-488](#)

show mac address-table address command [2-492](#)

show mac address-table aging time command [2-494](#)

show mac address-table command [2-490](#)

show mac address-table count command [2-496](#)

- show mac address-table dynamic command [2-498](#)
- show mac address-table interface command [2-500](#)
- show mac address-table learning command [2-502](#)
- show mac address-table move update [2-503](#)
- show mac address-table move update command [2-503](#)
- show mac address-table multicast command [2-505](#)
- show mac address-table notification command [2-48, 2-507, B-21](#)
- show mac address-table static command [2-509](#)
- show mac address-table vlan command [2-511](#)
- show mls qos aggregate-policer command [2-514](#)
- show mls qos command [2-513](#)
- show mls qos input-queue command [2-515](#)
- show mls qos interface command [2-517](#)
- show mls qos maps command [2-520](#)
- show mls qos queue-set command [2-523](#)
- show monitor command [2-526](#)
- show mvr command [2-532](#)
- show mvr interface command [2-534](#)
- show mvr members command [2-536](#)
- show pagp command [2-538](#)
- show parser macro command [2-540](#)
- show platform acl command [C-2](#)
- show platform cfm command [C-3](#)
- show platform configuration command [C-4](#)
- show platform etherchannel command [C-5](#)
- show platform forward command [C-6](#)
- show platform igmp snooping command [C-8](#)
- show platform ipc trace command [C-14](#)
- show platform ip multicast command [C-10](#)
- show platform ip policy command [C-11](#)
- show platform ip unicast command [C-12](#)
- show platform layer4op command [C-15](#)
- show platform mac-address-table command [C-16](#)
- show platform messaging command [C-17](#)
- show platform monitor command [C-18](#)
- show platform mvr table command [C-19](#)
- show platform pm command [C-20](#)
- show platform port-asic command [C-22](#)
- show platform port-security command [C-26](#)
- show platform qos command [C-27](#)
- show platform resource-manager command [C-28](#)
- show platform snmp counters command [C-30](#)
- show platform spanning-tree command [C-31](#)
- show platform stp-instance command [C-32](#)
- show platform tb command [C-33](#)
- show platform team command [C-34](#)
- show platform vlan command [C-37](#)
- show policy-map command [2-543](#)
- show port security command [2-546](#)
- show proposed command [2-724](#)
- show rep topology command [2-549](#)
- show sdm prefer command [2-551](#)
- show setup express command [2-553](#)
- show spanning-tree command [2-554](#)
- show storm-control command [2-560](#)
- show system mtu command [2-562](#)
- show trust command [2-700](#)
- show udd command [2-563](#)
- show version command [2-566](#)
- show vlan access-map command [2-573](#)
- show vlan command [2-568](#)
- show vlan command, fields [2-570](#)
- show vlan filter command [2-574](#)
- show vmps command [2-575](#)
- show vtp command [2-578](#)
- shutdown command [2-583](#)
- shutdown threshold, Layer 2 protocol tunneling [2-192](#)
- shutdown vlan command [2-584](#)
- small violation-rate command [2-585](#)
- Smartports macros
 - See macros
- SNMP host, specifying [2-592](#)
- SNMP informs, enabling the sending of [2-588](#)
- snmp mib rep trap-rate command [2-587](#)
- snmp-server enable traps command [2-588](#)
- snmp-server host command [2-592](#)
- snmp trap mac-notification command [2-597](#)

SNMP traps

- enabling MAC address notification trap [2-597](#)
- enabling the MAC address notification feature [2-220](#)
- enabling the sending of [2-588](#)

SoftPhone

- See Cisco SoftPhone

software images

- deleting [2-72](#)
- downloading [2-7](#)
- monitoring status of [2-392](#)
- upgrading [2-7](#)
- uploading [2-12](#)

software version, displaying [2-566](#)source ports, MVR [2-295](#)

SPAN

- configuring [2-283](#)
- debug messages, display [B-22](#)
- displaying [2-526](#)
- filter SPAN traffic [2-283](#)
- sessions
 - add interfaces to [2-283](#)
 - displaying [2-526](#)
 - start new [2-283](#)

spanning-tree backbonefast command [2-598](#)spanning-tree bpduguard command [2-599](#)spanning-tree bpduguard command [2-601](#)spanning-tree cost command [2-603](#)spanning-tree etherchannel command [2-605](#)spanning-tree extend system-id command [2-607](#)spanning-tree guard command [2-608](#)spanning-tree link-type command [2-610](#)spanning-tree loopguard default command [2-612](#)spanning-tree mode command [2-614](#)spanning-tree mst configuration command [2-616](#)spanning-tree mst cost command [2-618](#)spanning-tree mst forward-time command [2-620](#)spanning-tree mst hello-time command [2-621](#)spanning-tree mst max-age command [2-622](#)spanning-tree mst max-hops command [2-623](#)spanning-tree mst port-priority command [2-626](#)spanning-tree mst pre-standard command [2-625](#)spanning-tree mst priority command [2-628](#)spanning-tree mst root command [2-629](#)spanning-tree portfast (global configuration) command [2-633](#)spanning-tree portfast (interface configuration) command [2-635](#)spanning-tree port-priority command [2-631](#)

Spanning Tree Protocol

See STP

spanning-tree uplinkfast command [2-637](#)spanning-tree vlan command [2-639](#)speed command [2-642](#)srr-queue bandwidth limit command [2-644](#)srr-queue bandwidth shape command [2-646](#)srr-queue bandwidth share command [2-648](#)SSH, configuring version [2-181](#)static-access ports, configuring [2-655](#)statistics, Ethernet group [2-369](#)sticky learning, enabling [2-673](#)storm-control command [2-650](#)

STP

BackboneFast [2-598](#)counters, clearing [2-51](#)

debug messages, display

BackboneFast events [B-72](#)MSTP [B-75](#)optimized BPDUs handling [B-74](#)spanning-tree activity [B-70](#)switch shim [B-77](#)transmitted and received BPDUs [B-73](#)UplinkFast [B-79](#)detection of indirect link failures [2-598](#)enabling protocol tunneling for [2-192](#)EtherChannel misconfiguration [2-605](#)extended system ID [2-607](#)path cost [2-603](#)protocol modes [2-614](#)

STP (continued)

root port

- accelerating choice of new [2-637](#)
- loop guard [2-608](#)
- preventing from becoming designated [2-608](#)
- restricting which can be root [2-608](#)
- root guard [2-608](#)
- UplinkFast [2-637](#)

root switch

- affects of extended system ID [2-607, 2-640](#)
- hello-time [2-639](#)
- interval between BDPU messages [2-639](#)
- interval between hello BPDU messages [2-639](#)
- max-age [2-639](#)
- port priority for selection of [2-631](#)
- primary or secondary [2-639](#)
- switch priority [2-639](#)

state changes

- blocking to forwarding state [2-635](#)
- enabling BPDU filtering [2-599, 2-633](#)
- enabling BPDU guard [2-601, 2-633](#)
- enabling Port Fast [2-633, 2-635](#)
- enabling timer to recover from error state [2-108](#)
- forward-delay time [2-639](#)
- length of listening and learning states [2-639](#)
- shutting down Port Fast-enabled ports [2-633](#)

state information display [2-554](#)VLAN options [2-628, 2-639](#)SVIs, creating [2-126](#)

Switched Port Analyzer

See SPAN

switching characteristics

- modifying [2-653, 2-671](#)
- returning to interfaces [2-653, 2-671](#)

switchport access command [2-655](#)switchport backup interface command [2-657, 2-660](#)switchport block command [2-664](#)switchport command [2-653](#)switchport host command [2-665](#)switchport mode command [2-666](#)switchport mode private-vlan command [2-669](#)switchport nonegotiate command [2-671](#)switchport port-security aging command [2-677](#)switchport port-security command [2-673](#)switchport priority extend command [2-679](#)switchport private-vlan command [2-681](#)switchport protected command [2-683](#)switchports, displaying [2-437](#)switchport trunk command [2-684](#)switchport vlan mapping command [2-688](#)switchport voice vlan command [2-691](#)system message logging, save message to flash [2-209](#)system mtu command [2-693](#)system resource templates [2-370](#)

T
tar files, creating, listing, and extracting [2-9](#)Telnetting to cluster switches [2-350](#)temperature information, displaying [2-422](#)templates, system resources [2-370](#)traceroute mac command [2-695](#)traceroute mac ip command [2-698](#)trunking, VLAN mode [2-666](#)trunk mode [2-666](#)trunk ports [2-666](#)trunks, to non-DTP device [2-667](#)trusted boundary for QoS [2-279](#)trusted port states for QoS [2-279](#)

tunneling

drop threshold [2-194](#)PAgP, LACP, and UDLD packets [2-193](#)shutdown threshold [2-194](#)tunnel ports, Layer 2 protocol, displaying [2-478](#)type (boot loader) command [A-23](#)

U

UDLD

- aggressive mode [2-702, 2-704](#)
- debug messages, display [B-86](#)
- enable globally [2-702](#)
- enable per interface [2-704](#)
- error recovery timer [2-108](#)
- message timer [2-702](#)
- normal mode [2-702, 2-704](#)
- reset a shutdown interface [2-706](#)
- status [2-563](#)

udld (global configuration) command [2-702](#)

udld (interface configuration) command [2-704](#)

udld reset command [2-706](#)

UNI

- bundling and multiplexing [2-117](#)
- Ethernet [2-117](#)

unicast storm control [2-650](#)

uni count command [2-707](#)

UniDirectional Link Detection

See UDLD

UNI ID, Ethernet [2-119](#)

unknown multicast traffic, preventing [2-664](#)

unknown unicast traffic, preventing [2-664](#)

unset (boot loader) command [A-24](#)

upgrading, software images [2-7](#)

upgrading information

See release notes [xx](#)

UplinkFast, for STP [2-637](#)

user EXEC mode [1-2](#)

V

VCs

- assigning interfaces to [1-5, 2-741](#)
- configuring [2-287](#)
- MPLS, displaying [2-528](#)

version (boot loader) command [A-26](#)

virtual circuits

See VCs

VLAN

enabling guest VLAN supplicant [2-79](#)

vlan (global configuration) command [2-709](#)

vlan (VLAN configuration) command [2-715](#)

vlan access-map command [2-721](#)

VLAN access map configuration mode [2-721](#)

VLAN access maps

actions [2-5](#)

displaying [2-573](#)

VLAN-based QoS [2-282](#)

VLAN configuration

rules [2-712, 2-717](#)

saving [2-709, 2-719](#)

VLAN configuration mode

commands

VLAN [2-715](#)

VTP [2-737](#)

description [1-4](#)

entering [2-723](#)

summary [1-2](#)

vlan database command [2-723](#)

vlan filter command [2-726](#)

VLAN filters, displaying [2-574](#)

VLAN ID range [2-709, 2-715](#)

VLAN mapping, command [2-689](#)

VLAN maps

applying [2-726](#)

creating [2-721](#)

defining [2-235](#)

displaying [2-573](#)

VLAN Query Protocol

See VQP

VLANs

- adding [2-709](#)
- configuring [2-709, 2-715](#)
- debug messages, display
 - ISL [B-83](#)
 - VLAN IOS file system error tests [B-82](#)
 - VLAN manager activity [B-80](#)
 - VTP [B-84](#)
- displaying configurations [2-568](#)
- extended-range [2-709](#)
- MAC addresses
 - displaying [2-511](#)
 - number of [2-496](#)
- media types [2-712, 2-717](#)
- normal-range [2-709, 2-715](#)
- private [2-669](#)
 - configuring [2-329](#)
 - displaying [2-568](#)
 - See also private VLANs
- restarting [2-584](#)
- saving the configuration [2-709](#)
- shutting down [2-584](#)
- SNMP traps for VTP [2-590, 2-594](#)
- suspending [2-584](#)
- variables [2-715](#)

VLAN template [2-370](#)

VLAN Trunking Protocol

See VTP

VMPS

- configuring servers [2-731](#)
- displaying [2-575](#)
- error recovery timer [2-108](#)
- reconfirming dynamic VLAN assignments [2-728](#)
- vmmps reconfirm (global configuration) command [2-729](#)
- vmmps reconfirm (privileged EXEC) command [2-728](#)
- vmmps retry command [2-730](#)
- vmmps server command [2-731](#)

voice VLAN

- configuring [2-691](#)
- setting port priority [2-679](#)

VPN routing/forwarding table

See VRF

VQP

- and dynamic-access ports [2-655](#)
- clearing client statistics [2-53](#)
- displaying information [2-575](#)
- per-server retry count [2-730](#)
- reconfirmation interval [2-729](#)
- reconfirming dynamic VLAN assignments [2-728](#)

VRF

- associating to an interface [2-190](#)
- configuring [2-188](#)

VTP

- changing characteristics [2-733](#)
- clearing pruning counters [2-54](#)
- configuring
 - domain name [2-733, 2-737](#)
 - file name [2-733](#)
 - mode [2-733, 2-737](#)
 - password [2-733, 2-737](#)
- counters display fields [2-579](#)
- displaying information [2-578](#)
- enabling
 - pruning [2-733, 2-737](#)
 - tunneling for [2-192](#)
 - version 2 [2-733, 2-737](#)
- mode [2-733, 2-737](#)
- pruning [2-733, 2-737](#)
- saving the configuration [2-709, 2-719](#)
- statistics [2-578](#)
- status [2-578](#)
- status display fields [2-580](#)
- vtp (global configuration) command [2-733](#)
- vtp (VLAN configuration) command [2-737](#)

X

xconnect command [2-741](#)