



Catalyst 4500 Series Switch Cisco IOS Command Reference

Release 12.2(18)EW

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-7816201=
Text Part Number: 78-16201-01



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

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

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

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

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

CCDP, the Cisco Express Router logo, Cisco Unity, Follow Me Forwarding, Forwarders, and Standalone are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Advanced, ASIST, BPK, Catalyst, CE100, CE100P, CE100, CE100P, CE100A, CE100B, Cisco, the Cisco Certified Internetwork Expert logo, Cisco EEM, Cisco Express, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, EnterpriseVoice, EtherChannel, EtherFast, EtherSwitch, Fast Way, Gigaset, Gigaset, HomeLink, Internet Quantum, ISM, IPTV, IJ Register, the IJ logo, IJ Net Readiness Assessment, iLightView, Linksys, MeetingPlace, MESH, the Networker logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, PreConnect, RAINBOW, Registrar, ScriptCenter, SlideCast, SMARTnet, MetaView Plus, PacketPulse, TelePresence, The Fastest Way to Increase Your Internet Quantum, Thousand, and VCE 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. [000000]



Preface	xv
Audience	xv
Organization	xv
Related Documentation	xv
Conventions	xvi
Obtaining Documentation	xvii
Documentation Feedback	xviii
Obtaining Technical Assistance	xviii
Obtaining Additional Publications and Information	xix

CHAPTER 1

Command-Line Interface	1-1
Getting Help	1-1
How to Find Command Options	1-2
Understanding Command Modes	1-4
Using the No and Default Forms of Commands	1-6
Using the CLI String Search	1-6
Saving Configuration Changes	1-11
Show Platform Commands	1-11

CHAPTER 2

Cisco IOS Commands for the Catalyst 4500 Series Switches	2-1
#macro keywords	2-2
aaa accounting dot1x default start-stop group radius	2-3
aaa accounting system default start-stop group radius	2-4
access-group mode	2-5
action	2-6
apply	2-7
arp access-list	2-8
attach module	2-9
auto qos voip	2-10
auto-sync	2-13
channel-group	2-14
channel-protocol	2-16

class-map	2-18
clear counters	2-20
clear hw-module slot password	2-22
clear interface gigabitethernet	2-23
clear interface vlan	2-24
clear ip access-template	2-25
clear ip arp inspection log	2-26
clear ip arp inspection statistics	2-27
clear ip dhcp snooping database	2-28
clear ip dhcp snooping database statistics	2-29
clear ip igmp group	2-30
clear ip igmp snooping membership	2-32
clear ip mfib counters	2-33
clear ip mfib fastdrop	2-34
clear lacp counters	2-35
clear mac-address-table dynamic	2-36
clear pagp	2-37
clear port-security	2-38
clear qos	2-39
clear vlan counters	2-40
clear vmps statistics	2-41
debug adjacency	2-42
debug backup	2-43
debug condition interface	2-44
debug condition standby	2-45
debug condition vlan	2-47
debug dot1x	2-48
debug etherchnl	2-49
debug interface	2-51
debug ipc	2-52
debug ip dhcp snooping event	2-53
debug ip dhcp snooping packet	2-54
debug ip verify source packet	2-55
debug lacp	2-56
debug monitor	2-57

[debug nvram](#) 2-58

[debug pagp](#) 2-59

[debug platform packet protocol lacp](#) 2-60

[debug platform packet protocol pagp](#) 2-61

[debug pm](#) 2-62

[debug psecure](#) 2-63

[debug redundancy](#) 2-64

[debug smf updates](#) 2-65

[debug spanning-tree](#) 2-66

[debug spanning-tree backbonefast](#) 2-67

[debug spanning-tree switch](#) 2-68

[debug spanning-tree uplinkfast](#) 2-70

[debug sw-vlan](#) 2-71

[debug sw-vlan ifs](#) 2-72

[debug sw-vlan notification](#) 2-73

[debug sw-vlan vtp](#) 2-74

[debug udld](#) 2-75

[debug vqpc](#) 2-76

[define interface-range](#) 2-77

[deny](#) 2-78

[diagnostic monitor action](#) 2-80

[dot1x guest-vlan](#) 2-81

[dot1x initialize](#) 2-82

[dot1x max-reauth-req](#) 2-83

[dot1x max-req](#) 2-84

[dot1x multiple-hosts](#) 2-85

[dot1x port-control](#) 2-86

[dot1x re-authenticate](#) 2-88

[dot1x re-authentication](#) 2-89

[dot1x system-auth-control](#) 2-90

[dot1x timeout](#) 2-91

[duplex](#) 2-93

[errdisable detect](#) 2-95

[errdisable recovery](#) 2-97

[flowcontrol](#) 2-100

hw-module power	2-103
instance	2-104
interface port-channel	2-107
interface range	2-108
interface vlan	2-110
ip arp inspection filter vlan	2-111
ip arp inspection limit (interface)	2-113
ip arp inspection log-buffer	2-115
ip arp inspection trust	2-117
ip arp inspection validate	2-118
ip arp inspection vlan	2-120
ip arp inspection vlan logging	2-121
ip cef load-sharing algorithm	2-123
ip dhcp snooping	2-124
ip dhcp snooping binding	2-125
ip dhcp snooping database	2-126
ip dhcp snooping information option	2-128
ip dhcp snooping limit rate	2-129
ip dhcp snooping trust	2-130
ip dhcp snooping vlan	2-131
ip igmp filter	2-133
ip igmp max-groups	2-134
ip igmp profile	2-135
ip igmp query-interval	2-136
ip igmp snooping	2-137
ip igmp snooping report-suppression	2-139
ip igmp snooping vlan	2-141
ip igmp snooping vlan explicit-tracking	2-142
ip igmp snooping vlan immediate-leave	2-143
ip igmp snooping vlan mrouter	2-144
ip igmp snooping vlan static	2-146
ip local-proxy-arp	2-147
ip mfib fastdrop	2-148
ip route-cache flow	2-149
ip source binding	2-151

ip sticky-arp	2-152
ip verify header vlan all	2-154
ip verify source vlan dhcp-snooping	2-155
l2protocol-tunnel	2-157
l2protocol-tunnel cos	2-158
l2protocol-tunnel drop-threshold	2-159
l2protocol-tunnel shutdown-threshold	2-160
lACP port-priority	2-161
lACP system-priority	2-162
mac access-list extended	2-163
mac-address-table aging-time	2-166
mac-address-table dynamic group protocols	2-167
mac-address-table static	2-170
macro apply cisco-desktop	2-172
macro apply cisco-phone	2-174
macro apply cisco-router	2-176
macro apply cisco-switch	2-178
main-cpu	2-180
match	2-181
monitor session	2-182
mtu	2-186
name	2-187
pagp learn-method	2-188
pagp port-priority	2-189
permit	2-190
policy-map	2-192
port-channel load-balance	2-194
power dc input	2-196
power inline	2-197
power inline consumption	2-199
power redundancy-mode	2-200
power supplies required	2-202
private-vlan	2-203
private-vlan mapping	2-205
private-vlan synchronize	2-207

qos (global configuration mode)	2-208
qos (interface configuration mode)	2-209
qos account layer2 encapsulation	2-210
qos aggregate-policer	2-212
qos cos	2-215
qos dbl	2-216
qos dscp	2-218
qos map cos	2-219
qos map dscp	2-220
qos map dscp policed	2-222
qos rewrite ip dscp	2-223
qos trust	2-224
qos vlan-based	2-226
redundancy	2-227
redundancy force-switchover	2-228
redundancy reload	2-229
remote login module	2-230
remote-span	2-231
renew ip dhcp snooping database	2-232
reset	2-233
revision	2-234
service-policy	2-235
session module	2-236
shape	2-237
show access-group mode interface	2-239
show arp access-list	2-240
show auto qos	2-241
show bootflash:	2-243
show bootvar	2-245
show class-map	2-246
show diagnostic result module	2-247
show diagnostic result module test 2	2-251
show diagnostic result module test 3	2-253
show dot1x	2-255
show environment	2-258

[show errdisable detect](#) 2-261

[show errdisable recovery](#) 2-262

[show etherchannel](#) 2-263

[show flowcontrol](#) 2-267

[show idprom](#) 2-269

[show interfaces](#) 2-274

[show interfaces capabilities](#) 2-276

[show interfaces counters](#) 2-279

[show interfaces description](#) 2-281

[show interfaces link](#) 2-282

[show interfaces mtu](#) 2-283

[show interfaces private-vlan mapping](#) 2-284

[show interfaces status](#) 2-285

[show interfaces switchport](#) 2-286

[show interfaces transceiver](#) 2-288

[show interfaces trunk](#) 2-293

[show ip arp inspection](#) 2-295

[show ip arp inspection log](#) 2-298

[show ip cef vlan](#) 2-299

[show ip dhcp snooping](#) 2-300

[show ip dhcp snooping binding](#) 2-301

[show ip dhcp snooping database](#) 2-304

[show ip igmp interface](#) 2-306

[show ip igmp profile](#) 2-307

[show ip igmp snooping](#) 2-308

[show ip igmp snooping membership](#) 2-312

[show ip igmp snooping mrouter](#) 2-314

[show ip igmp snooping vlan](#) 2-315

[show ip mfib](#) 2-316

[show ip mfib fastdrop](#) 2-318

[show ip mroute](#) 2-319

[show ip source binding](#) 2-324

[show ip verify source](#) 2-325

[show ipc](#) 2-327

[show l2protocol-tunnel](#) 2-329

show lacp 2-332

show mac access-group interface 2-335

show mac-address-table address 2-336

show mac-address-table aging-time 2-338

show mac-address-table count 2-339

show mac-address-table dynamic 2-340

show mac-address-table interface 2-342

show mac-address-table multicast 2-344

show mac-address-table protocol 2-346

show mac-address-table static 2-348

show mac-address-table vlan 2-350

show module 2-352

show monitor 2-354

show pagp 2-356

show policy-map 2-358

show policy-map interface 2-359

show port-security 2-361

show power 2-363

show qos 2-367

show qos aggregate policer 2-368

show qos dbl 2-369

show qos interface 2-370

show qos maps 2-371

show redundancy 2-373

show running-config 2-376

show slavebootflash: 2-378

show slaveslot0: 2-380

show slot0: 2-382

show spanning-tree 2-384

show spanning-tree mst 2-389

show storm-control 2-391

show system mtu 2-393

show tech-support 2-394

show udld 2-396

show vlan 2-397

show vlan access-map	2-400
show vlan counters	2-401
show vlan dot1q tag native	2-402
show vlan internal usage	2-403
show vlan mtu	2-404
show vlan private-vlan	2-405
show vlan remote-span	2-407
show vmps	2-408
show vtp	2-409
snmp ifindex clear	2-413
snmp ifindex persist	2-414
snmp-server enable traps	2-415
snmp-server ifindex persist	2-417
snmp-server ifindex persist compress	2-418
spanning-tree backbonefast	2-419
spanning-tree bpdupfilter	2-420
spanning-tree bpduguard	2-422
spanning-tree cost	2-423
spanning-tree etherchannel guard misconfig	2-424
spanning-tree extend system-id	2-425
spanning-tree guard	2-426
spanning-tree link-type	2-427
spanning-tree loopguard default	2-428
spanning-tree mode	2-429
spanning-tree mst	2-430
spanning-tree mst configuration	2-431
spanning-tree mst forward-time	2-433
spanning-tree mst hello-time	2-434
spanning-tree mst max-age	2-435
spanning-tree mst max-hops	2-436
spanning-tree mst root	2-437
spanning-tree pathcost method	2-439
spanning-tree portfast (interface configuration mode)	2-440
spanning-tree portfast bpdupfilter default	2-442
spanning-tree portfast bpduguard default	2-444

spanning-tree portfast default	2-445
spanning-tree port-priority	2-446
spanning-tree uplinkfast	2-447
spanning-tree vlan	2-449
speed	2-451
storm-control	2-454
storm-control broadcast include multicast	2-456
switchport	2-457
switchport access vlan	2-459
switchport block	2-461
switchport mode	2-462
switchport port-security	2-464
switchport private-vlan association trunk	2-468
switchport private-vlan host-association	2-469
switchport private-vlan mapping	2-470
switchport private-vlan trunk allowed vlan	2-471
switchport private-vlan trunk native vlan	2-473
switchport trunk	2-474
system mtu	2-477
traceroute mac	2-478
traceroute mac ip	2-481
tx-queue	2-484
udld (global configuration mode)	2-486
udld (interface configuration mode)	2-488
udld reset	2-490
unidirectional	2-491
username	2-492
verify	2-493
vlan (VLAN Database mode)	2-495
vlan access-map	2-498
vlan database	2-499
vlan dot1q tag native	2-501
vlan filter	2-502
vlan internal allocation policy	2-503
vmps reconfirm (global configuration)	2-504

vmps reconfirm (privileged EXEC)	2-505
vmps retry	2-506
vmps server	2-507
vtp (global configuration mode)	2-509
vtp client	2-510
vtp domain	2-511
vtp password	2-512
vtp pruning	2-513
vtp server	2-514
vtp transparent	2-515
vtp v2-mode	2-516

INDEX

APPENDIX A**Acronyms** A-1

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



Preface

This preface describes the audience, organization, and conventions of this publication, and provides information on how to obtain related documentation.

Audience

This publication is for experienced network administrators who are responsible for configuring and maintaining Catalyst4500 series switches.

Organization

This publication is organized as follows:

Chapter	Title	Description
Chapter 1	Command-Line Interface	Describes the Catalyst4500 series switch CLI.
Chapter 2	Cisco IOS Commands for the Catalyst 4500 Series Switches	Lists all Catalyst4500 series CiscoIOS commands alphabetically and provides detailed information on each command.
Appendix A	Acronyms	Defines the acronyms used in this publication.
Appendix B	Acknowledgments for Open-Source Software	Provides the acknowledgments for Open-Source Software.

Related Documentation

The Catalyst4500 series Cisco IOS documentation set includes these publications:

- *Catalyst4500 Series Switch InstallationGuide*
- *Catalyst 4500 Series Switch Supervisor Engine III Installation Note*
- *Catalyst 4500 Series Switch Supervisor Engine IV Installation Note*
- *Catalyst4500 Series Switch Cisco IOS Software Configuration Guide*

- *Catalyst4500 Series Switch Cisco IOS System Message Guide*
- *Release Notes for Catalyst 4500 Series Switch Software Release 12.1(13)EW*

Other documents in the Cisco IOS documentation set include:

- *Cisco IOS Release 12.1 Configuration Guides*
- *Cisco IOS Release 12.1 Command References*

For information about MIBs, refer to this URL:

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

Conventions

This document uses these conventions:

Convention	Description
boldface font	Boldface text indicates commands and keywords that you enter literally as shown.
<i>italic font</i>	<i>Italic</i> text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional element (keyword or argument).
	A vertical line indicates a choice within an optional or required set of keywords or arguments.
[x y]	Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.
{x y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.
[x {y z}]	Braces and a vertical line within square brackets indicate a required choice within an optional element.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
screen font	Terminal sessions and information the system displays are in screen font.
boldface screen font	Information you must enter is in boldface screen font .
<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screen font</i> .
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets.

Convention	Description
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Notes use this convention:



Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Cautions use this convention:



Caution

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

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408526-7208 or, elsewhere in North America, by calling 800553-NETS (6387).

Documentation Feedback

You can submit e-mail comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year. The Cisco TAC website is located at this URL:

<http://www.cisco.com/tac>

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

<http://www.cisco.com/tac/caseopen>

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Go to this URL to visit the company store:
<http://www.cisco.com/go/marketplace/>
- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:
<http://cisco.com/univercd/cc/td/doc/pcat/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press online at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>

- *iQ Magazine* is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:
<http://www.cisco.com/en/US/learning/index.html>



Command-Line Interface

This chapter provides information for understanding and using the Cisco IOS command-line interface (CLI) on the Catalyst4500 series switch. This chapter includes the following sections:

- [Getting Help, page 1-1](#)
- [How to Find Command Options, page 1-2](#)
- [Understanding Command Modes, page 1-4](#)
- [Using the No and Default Forms of Commands, page 1-6](#)
- [Using the CLI String Search, page 1-6](#)
- [Saving Configuration Changes, page 1-11](#)

For an overview of the Catalyst4500 series switch Cisco IOS configuration, refer to the *Catalyst4500 Series Switch Cisco IOS Software Configuration Guide*.

Getting Help

To display a list of commands that you can use within a command mode, enter a question mark (?) at the system prompt. You also can display keywords and arguments for each command with this context-sensitive help feature.

Table 1-1 lists commands you can enter to get help that is specific to a command mode, a command, a keyword, or an argument.

Table 1-1 Getting Help

Command	Purpose
<i>abbreviated-command-entry?</i>	Displays a list of commands that begin with a particular character string. (Do not leave a space between the command and question mark.)
<i>abbreviated-command-entry</i> <Tab>	Completes a partial command name.
?	Lists all commands for the command mode.
<i>command ?</i>	Lists all keywords for the command. Leave a space between the command and the question mark.
<i>command keyword ?</i>	Lists all arguments for the keyword. Leave a space between the keyword and the question mark.

How to Find Command Options

This section provides an example of how to display syntax for a command. The syntax can consist of optional or required keywords. To display keywords for a command, enter a question mark (?) at the command prompt or after entering part of a command followed by a space. The Catalyst4500 series switch software displays a list of available keywords along with a brief description of the keywords. For example, if you are in global configuration mode and want to see all the keywords for the **arap** command, you enter **arap ?**.

Table1-2 shows examples of how you can use the question mark (?) to assist you in entering commands and also guides you through entering the following commands:

- **interface gigabitethernet 1/1**
- **channel-group 1 mode auto**

Table1-2 How to Find Command Options

Command	Purpose
Switch> enable Password: <password> Switch#	Enter the enable command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to Switch#.
Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#	Enter global configuration mode. You are in global configuration mode when the prompt changes to Switch(config)#.
Switch(config)# interface gigabitethernet ? <1-9> GigabitEthernet interface number Switch(config)# interface gigabitethernet 1/1 Switch(config-if)#	Enter interface configuration mode by specifying the Gigabit Ethernet interface that you want to configure using the interface gigabitethernet global configuration command. Enter a ? to display what you must enter next on the command line. In this example, you must enter an interface number from 1 to 9 in the format <i>module-number/port-number</i> . You are in interface configuration mode when the prompt changes to Switch(config-if)#.

Table1-2 How to Find Command Options (continued)

Command	Purpose
<pre>Switch(config-if)#? Interface configuration commands: access-expression Build a bridge boolean access expression apollo Apollo interface subcommands appletalk Appletalk interface subcommands arp Set arp type (arpa, probe, snap) or timeout backup Modify backup parameters bandwidth Set bandwidth informational parameter bgp-policy Apply policy propogated by bgp community string bridge-group Transparent bridging interface parameters carrier-delay Specify delay for interface transitions cdp CDP interface subcommands channel-group Etherchannel/port bundling configuration clns CLNS interface subcommands cmns OSI CMNS custom-queue-list Assign a custom queue list to an interface decnet Interface DECnet config commands default Set a command to its defaults delay Specify interface throughput delay description Interface specific description dlsw DLSw interface subcommands dspu Down Stream PU exit Exit from interface configuration mode fair-queue Enable Fair Queuing on an Interface flowcontrol Configure flow operation. fras DLC Switch Interface Command help Description of the interactive help system hold-queue Set hold queue depth ip Interface Internet Protocol config commands ipx Novell/IPX interface subcommands isis IS-IS commands iso-igrp ISO-IGRP interface subcommands . . .</pre>	<p>Enter a ? to display a list of all the interface configuration commands available for the Gigabit Ethernet interface.</p>
<pre>Switch(config-if)# Switch(config-if)# channel-group ? group channel-group of the interface Switch(config-if)#channel-group</pre>	<p>Enter the command that you want to configure for the controller. In this example, the channel-group command is used.</p> <p>Enter a ? to display what you must enter next on the command line. In this example, you must enter the group keyword.</p> <p>Because a <cr> is not displayed, it indicates that you must enter more information to complete the command.</p>

Table1-2 How to Find Command Options (continued)

Command	Purpose
<pre>Switch(config-if)# channel-group ? <1-256> Channel group number Switch(config-if)#channel-group</pre>	<p>After you enter the group keyword, enter a ? to display what you must enter next on the command line. In this example, you must enter a channel group number from 1 to 256.</p> <p>Because a <code><cr></code> is not displayed, it indicates that you must enter more information to complete the command.</p>
<pre>Switch(config-if)# channel-group 1 ? mode Etherchannel Mode of the interface Switch(config-if)#</pre>	<p>After you enter the channel group number, enter a ? to display what you must enter next on the command line. In this example, you must enter the mode keyword.</p> <p>Because a <code><cr></code> is not displayed, it indicates that you must enter more information to complete the command.</p>
<pre>Switch(config-if)# channel-group 1 mode ? auto Enable PAgP only if a PAgP device is detected desirable Enable PAgP unconditionally on Enable Etherchannel only Switch(config-if)#</pre>	<p>After you enter the mode keyword, enter a ? to display what you must enter next on the command line. In this example, you must enter the auto, desirable, or on keyword.</p> <p>Because a <code><cr></code> is not displayed, it indicates that you must enter more information to complete the command.</p>
<pre>Switch(config-if)# channel-group 1 mode auto ? <cr> Switch(config-if)#</pre>	<p>In this example, the auto keyword is entered. After you enter the auto keyword, enter a ? to display what you must enter next on the command line.</p> <p>Because a <code><cr></code> is displayed, it indicates that you can press Return to complete the command. If additional keywords are listed, you can enter more keywords or press Return to complete the command.</p>
<pre>Switch(config-if)# channel-group 1 mode auto Switch(config-if)#</pre>	<p>In this example, press Return to complete the command.</p>

Understanding Command Modes

The CiscoIOS user interface on the Catalyst4500 series switch has many different modes. The commands that are available to you depend on which mode you are currently in. You can obtain a list of commands available for each command mode by entering a question mark (?) at the system prompt.

When you start a session on the Catalyst4500 series switch, you begin in user mode, often called EXEC mode. Only a limited subset of the commands are available in EXEC mode. In order to have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From privileged EXEC mode, you can enter any EXEC command or enter global configuration mode. Most EXEC commands are one-time commands, such as **show** commands, which show the current status of a given item, and **clear** commands, which clear counters or interfaces. The EXEC commands are not saved across reboots of the Catalyst4500 series switch.

The configuration modes provide a way for you to make changes to the running configuration. When you save changes to the configuration, the changes remain intact when the Catalyst 4500 series switch reboots. From global configuration mode, you can enter interface configuration mode, subinterface configuration mode, and other protocol-specific modes.

ROM-monitor mode is a separate mode used when the Catalyst4500 series switch cannot boot properly. If your Catalyst4500 series switch or access server does not find a valid system image when it is booting, or if its configuration file is corrupted at startup, the system might enter ROM-monitor mode.

Table 1-3 provides a summary of the main command modes.

Table 1-3 Summary of Main Command Modes

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in.	Switch>	Use the logout command.
Privileged EXEC	From user EXEC mode, enter the enable EXEC command.	Switch#	To exit to user EXEC mode, enter the disable command. To enter global configuration mode, enter the configure terminal privileged EXEC command.
Global configuration	From privileged EXEC mode, enter the configure terminal privileged EXEC 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 an interface configuration command.
Interface configuration	From global configuration mode, enter by specifying an interface with an interface command.	Switch(config-if)#	To exit to global configuration mode, enter the exit command. To exit to privileged EXEC mode, enter the exit command or press Ctrl-Z . To enter subinterface configuration mode, specify a subinterface with the interface command.

Table1-3 Summary of Main Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method
Subinterface configuration	From interface configuration mode, specify a subinterface with an interface command.	Switch(config-subif)#	To exit to global configuration mode, enter the exit command. To enter privileged EXEC mode, enter the end command or press Ctrl-Z .
ROM monitor	From privileged EXEC mode, enter the reload EXEC command. Press the Break key during the first 60 seconds while the system is booting.	Rommon>	To exit ROM-monitor mode, you must reload the image by entering the boot command. If you use the boot command without specifying a file or any other boot instructions, the system boots from the default Flash image (the first image in onboard Flash memory). Otherwise, you can instruct the system to boot from a specific Flash image (using the boot system flash filename command).

For more information on command modes, refer to the “Using the Command Line Interface” chapter of the *Configuration Fundamentals Configuration Guide*.

Using the No and Default Forms of Commands

Almost every configuration command has a **no** form. In general, enter the **no** form to disable a function. Use the command without the keyword **no** to reenable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, specify the **no iprouting** command and specify **ip routing** to reenable it. This publication provides the complete syntax for the configuration commands and describes what the **no** form of a command does.

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

Using the CLI String Search

The pattern in the command output is referred to as a string. The CLI string search feature allows you to search or filter any **show** or **more** command output and allows you to search and filter at --More-- prompts. This feature is useful when you need to sort through large amounts of output, or if you want to exclude output that you do not need to see.

With the search function, you can begin unfiltered output at the first line that contains a regular expression you specify. You can then specify a maximum of one filter per command or start a new search from the --More-- prompt.

A regular expression is a pattern (a phrase, number, or more complex pattern) software uses to match against **show** or **more** command output. Regular expressions are case sensitive and allow for complex matching requirements. Examples of simple regular expressions are Serial, misses, and 138. Examples of complex regular expressions are 00210..., (is), and [Oo]utput.

You can perform three types of filtering:

- Use the **begin** keyword to begin output with the line that contains a specified regular expression.
- Use the **include** keyword to include output lines that contain a specified regular expression.
- Use the **exclude** keyword to exclude output lines that contain a specified regular expression.

You can then search this filtered output at the --More-- prompts.



Note

The CLI string search function does not allow you to search or filter backward through previous output; filtering cannot be specified using HTTP access to the CLI.

Regular Expressions

A regular expression can be a single character that matches the same single character in the command output or multiple characters that match the same multiple characters in the command output. This section describes how to create both single-character patterns and multiple-character patterns and how to create more complex regular expressions using multipliers, alternation, anchoring, and parentheses.

Single-Character Patterns

The simplest regular expression is a single character that matches the same single character in the command output. You can use any letter (A-Z, a-z) or digit (0-9) as a single-character pattern. You can also use other keyboard characters (such as ! or ~) as single-character patterns, but certain keyboard characters have special meaning when used in regular expressions. [Table 1-4](#) lists the keyboard characters that have special meaning.

Table 1-4 Characters with Special Meaning

Character	Special Meaning
.	Matches any single character, including white space.
*	Matches 0 or more sequences of the pattern.
+	Matches 1 or more sequences of the pattern.
?	Matches 0 or 1 occurrences of the pattern.
^	Matches the beginning of the string.
\$	Matches the end of the string.
_ (underscore)	Matches a comma (,), left brace ({), right brace (}), left parenthesis ((), right parenthesis ()), the beginning of the string, the end of the string, or a space.

To enter these special characters as single-character patterns, remove the special meaning by preceding each character with a backslash (\). These examples are single-character patterns matching a dollar sign, an underscore, and a plus sign, respectively.

```
\$ \_ \+
```

You can specify a range of single-character patterns to match against command output. For example, you can create a regular expression that matches a string containing one of the following letters: a, e, i, o, or u. One and only one of these characters must exist in the string for pattern matching to succeed. To specify a range of single-character patterns, enclose the single-character patterns in square brackets ([]). For example,

[aeiou]

matches any one of the five vowels of the lowercase alphabet, while

[abcdABCD]

matches any one of the first four letters of the lower- or uppercase alphabet.

You can simplify ranges by entering only the end points of the range separated by a dash (-). Simplify the previous range as follows:

[a-dA-D]

To add a dash as a single-character pattern in your range, include another dash and precede it with a backslash:

[a-dA-D\ -]

You can also include a right square bracket (]) as a single-character pattern in your range. To do so, enter the following:

[a-dA-D\ -])]

The previous example matches any one of the first four letters of the lower- or uppercase alphabet, a dash, or a right square bracket.

You can reverse the matching of the range by including a caret (^) at the start of the range. This example matches any letter except the ones listed:

[^a-dqsv]

This example matches anything except a right square bracket (]) or the letter d:

[^\d]

Multiple-Character Patterns

When creating regular expressions, you can also specify a pattern containing multiple characters. You create multiple-character regular expressions by joining letters, digits, or keyboard characters that do not have special meaning. For example, a4% is a multiple-character regular expression. Put a backslash in front of the keyboard characters that have special meaning when you want to remove their special meaning.

With multiple-character patterns, order is important. The regular expression a4% matches the character a followed by a 4 followed by a % sign. If the string does not have a4%, in that order, pattern matching fails. This multiple-character regular expression:

a.

uses the special meaning of the period character to match the letter a followed by any single character. With this example, the strings ab, a!, or a2 are all valid matches for the regular expression.

You can remove the special meaning of the period character by putting a backslash in front of it. In the following expression:

a\.

only the string a. matches this regular expression.

You can create a multiple-character regular expression containing all letters, all digits, all keyboard characters, or a combination of letters, digits, and other keyboard characters. These examples are all valid regular expressions:

telebit 3107 v32bis

Multipliers

You can create more complex regular expressions to match multiple occurrences of a specified regular expression by using some special characters with your single- and multiple-character patterns. [Table 1-5](#) lists the special characters that specify “multiples” of a regular expression.

Table 1-5 Special Characters Used as Multipliers

Character	Description
*	Matches 0 or more single- or multiple-character patterns.
+	Matches 1 or more single- or multiple-character patterns.
?	Matches 0 or 1 occurrences of the single- or multiple-character patterns.

This example matches any number of occurrences of the letter a, including none:

a*

This pattern requires that at least one letter a in the string is matched:

a+

This pattern matches the string bb or bab:

ba?b

This string matches any number of asterisks (*):

To use multipliers with multiple-character patterns, you enclose the pattern in parentheses. In the following example, the pattern matches any number of the multiple-character string ab:

(ab)*

As a more complex example, this pattern matches one or more instances of alphanumeric pairs (but not none; that is, an empty string is not a match):

([A-Za-z][0-9])+

The order for matches using multipliers (*, +, or ?) is to put the longest construct first. Nested constructs are matched from outside to inside. Concatenated constructs are matched beginning at the left side of the construct. Thus, the regular expression matches A9b3, but not 9Ab3 because the letters are specified before the numbers.

Alternation

Alternation allows you to specify alternative patterns to match against a string. You separate the alternative patterns with a vertical bar (|). Exactly one of the alternatives can match the string. For example, the regular expression

codex | telebit

matches the string codex or the string telebit, but not both codex and telebit.

Anchoring

You can match a regular expression pattern against the beginning or the end of the string. That is, you can specify that the beginning or end of a string contains a specific pattern. You “anchor” these regular expressions to a portion of the string using the special characters shown in [Table1-6](#).

Table1-6 Special Characters Used for Anchoring

Character	Description
<code>^</code>	Matches the beginning of the string.
<code>\$</code>	Matches the end of the string.

This regular expression matches a string only if the string starts with `abcd`:

`^abcd`

In contrast, this expression is in a range that matches any single letter, as long as it is not the letters `a`, `b`, `c`, or `d`:

`[^abcd]`

With this example, the regular expression matches a string that ends with `.12`:

`$.12`

Contrast these anchoring characters with the special character underscore (`_`). The underscore matches the beginning of a string (`^`), the end of a string (`$`), parentheses (`()`), space (), braces (`{ }`), comma (`,`), or underscore (`_`). With the underscore character, you can specify that a pattern exist anywhere in the string.

For example:

`_1300_`

matches any string that has `1300` somewhere in the string. The string’s `1300` can be preceded by or end with a space, brace, comma, or underscore. For example:

`{1300_`

matches the regular expression, but `21300` and `13000` do not.

Using the underscore character, you can replace long regular expression lists, such as the following:

`^1300$ ^1300(space) (space)1300 {1300, ,1300, {1300} ,1300, (1300`

with

`_1300_`

Parentheses for Recall

As shown in the “[Multipliers](#)” section on [page1-9](#), you use parentheses with multiple-character regular expressions to multiply the occurrence of a pattern. You can also use parentheses around a single- or multiple-character pattern to remember a pattern for use elsewhere in the regular expression.

To create a regular expression that recalls a previous pattern, you use parentheses to indicate a remembered specific pattern and a backslash (`\`) followed by an integer to reuse the remembered pattern. The integer specifies the occurrence of the parentheses in the regular expression pattern. If you have more than one remembered pattern in your regular expression, then `\1` indicates the first remembered pattern, `\2` indicates the second remembered pattern, and so on.

This regular expression uses parentheses for recall:

```
a(.)bc(.)\1\2
```

This regular expression matches an a followed by any character (call it character 1), followed by bc followed by any character (character 2), followed by character 1 again, followed by character 2 again. So, the regular expression can match aZbcTZT. The software remembers that character 1 is Z and character 2 is T and then uses Z and T again later in the regular expression.

Saving Configuration Changes

To save your configuration changes to your startup configuration so that they will not be lost if there is a system reload or power outage, enter the following command:

```
Switch# copy system:running-config nvram:startup-config
Building configuration...
```

It might take a minute or two to save the configuration. After the configuration has been saved, the following output appears:

```
[OK]
Switch#
```

On most platforms, this step saves the configuration to NVRAM. On the Class A Flash file system platforms, this step saves the configuration to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE environment variable defaults to NVRAM.

Show Platform Commands

You should use these commands only when you are working directly with your technical support representative, while troubleshooting a problem. Do not use these commands unless your technical support representative asks you to do so.



Note

The **show platform** commands are not described in this document.



Cisco IOS Commands for the Catalyst 4500 Series Switches

This chapter contains an alphabetical listing of CiscoIOS commands for the Catalyst4500 series switches. For information about Cisco IOS commands that are not included in this publication, refer to CiscoIOS Release 12.1 ConfigurationGuides and CommandReferences at this URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_product_indices_list.html

#macro keywords

To specify the help string for macro keywords, use the **#macro keywords** command.

#macro keywords [keyword1] [keyword2] [keyword3]

Syntax Description	keyword 1	(Optional) Specifies a keyword that is needed while applying a macro to an interface.
	keyword 2	(Optional) Specifies a keyword that is needed while applying a macro to an interface.
	keyword 3	(Optional) Specifies a keyword that is needed while applying a macro to an interface.

Defaults This command has no default settings.

Command Modes Global configuration

Command History	Release	Modification
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines If you do not specify the mandatory keywords for a macro, the macro is to be considered invalid and fails when you attempt to apply it. By entering **#macro keywords**, you will receive a message indicating what you need to include to make the syntax valid.

Examples This example shows how to specify the help string for keywords associated with a macro named test:

```
Switch(config)# macro name test
macro name test
Enter macro commands one per line. End with the character '@'.
#macro keywords $VLAN $MAX
swichport
@

Switch(config)# int gil/1
Switch(config-if)# macro apply test ?
WORD Keyword to replace with a value e.g $VLAN, $MAX << It is shown as help
<cr>
```

Related Commands

- [macro apply cisco-desktop](#)
- [macro apply cisco-phone](#)
- [macro apply cisco-router](#)
- [macro apply cisco-switch](#)

aaa accounting dot1x default start-stop group radius

To enable accounting for dot.1x authentication sessions, use the **aaa accounting dot1x default start-stop group radius** command. Use the **no** form of this command to disable accounting.

aaa accounting dot1x default start-stop group radius

no aaa accounting dot1x default start-stop group radius

Syntax Description This command has no arguments or keywords.

Defaults Accounting is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines 802.1x accounting requires a RADIUS server.

This command enables the Authentication, Authorization, and Accounting (AAA) client's accounting feature to forward 802.1x update and watchdog packets from the 802.1x supplicant (workstation client) to the authentication (RADIUS) server. (Watchdog packets are defined as EAPOL-LOGON, EAPOL-LOGOFF, and EAPOL-INTERIM messages.) Successful authentication and authorization of the supplicant by the authentication server is required before these packets are considered valid and are forwarded. When the client is reauthenticated, an interim-update accounting notice is sent to the accounting server.

Examples The following example shows how to configure 802.1x accounting:

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



Note

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

Related Commands [aaa accounting system default start-stop group radius](#)

aaa accounting system default start-stop group radius

To receive session termination messages after the switch reboots, use the **aaa accounting system default start-stop group radius** command. Use the **no** form of this command to disable accounting.

aaa accounting system default start-stop group radius

no aaa accounting system default start-stop group radius

Syntax Description This command has no arguments or keywords.

Defaults Accounting is disabled.

Command Modes Global configuration mode

Command History	Release	Modification
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines 802.1x accounting requires the RADIUS server.

This command enables the AAA client's accounting feature to forward 802.1x update and watchdog packets from the 802.1x supplicant (workstation client) to the authentication (RADIUS) server. (Watchdog packets are defined as EAPOL-LOGON, EAPOL-LOGOFF, and EAPOL-INTERIM messages.) Successful authentication and authorization of the supplicant by the authentication server is required before these packets are considered valid and are forwarded. When the client is reauthenticated, an interim-update accounting notice is sent to the accounting server.

Examples The following example shows how to generate a logoff after a switch reboots:

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



Note

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

Related Commands [aaa accounting dot1x default start-stop group radius](#)

access-group mode

To specify override modes (for example, VACL overrides PACL) and non-override modes (for example, merge or strict mode), use the **access-group mode** command. Use the **no** form of this command to return to preferred port mode.

```
access-group mode {prefer {port | vlan} | merge }
```

```
no access-group mode {prefer {port | vlan} | merge }
```

Syntax Description

prefer port	Specifies that the PACL mode take precedence if PACLs are configured. If no PACL features are configured on the port, other features applicable to the interface are merged and applied on the interface.
prefer vlan	Specifies that the VLAN-based ACL mode take precedence. If no VLAN-based ACL features are configured on the port's VLAN, the PACL features on the port are applied.
merge	Merges applicable ACL features before they are programmed into the hardware .

Defaults

PACL override mode

Command Modes

Interface configuration

Command History

Release	Modification
12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

On the Layer 2 interface, prefer port, prefer VLAN, and merge modes are supported. A Layer2 interface can have one IP ACL applied in either direction (one inbound and one outbound).

Examples

This example shows how to make the PACL mode on the switch take effect:

```
(config-if)# access-group mode prefer port
```

This example shows how to merge applicable ACL features:

```
(config-if)# access-group mode merge
```

Related Commands

[show access-group mode interface](#)
[show ip interface](#) (refer to Cisco IOS documentation)
[show mac access-group interface](#)

action

To specify an action to be taken when a match occurs in a VACL, use the **action** command. To remove an action clause, use the **no** form of this command.

action {drop | forward }

no action {drop | forward }

Syntax Description

drop	Sets the action to drop packets.
forward	Sets the action to forward packets to their destination.

Defaults

This command has no default settings.

Command Modes

VLAN access-map

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

In a VLAN access map, if at least one ACL is configured for a packet type (IP or MAC), the default action for the packet type is **drop** (deny).

If an ACL is not configured for a packet type, the default action for the packet type is **forward** (permit).

If an ACL for a packet type is configured and the ACL is empty or undefined, the configured action will be applied to the packet type.

Examples

This example shows how to define a drop action:

```
Switch(config-access-map)# action drop
Switch(config-access-map)#
```

This example shows how to define a forward action:

```
Switch(config-access-map)# action forward
Switch(config-access-map)#
```

Related Commands

[match](#)
[show vlan access-map](#)
[vlan access-map](#)

apply

To implement a new VLAN database, increment the configuration number, save the configuration number in NVRAM, and propagate the configuration number throughout the administrative domain, use the **apply** command.

apply

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes VLAN configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines The **apply** command implements the configuration changes you made after you entered VLAN database mode and uses them for the running configuration. This command keeps you in VLAN database mode. You cannot use this command when the switch is in the VTP client mode.

You can verify that VLAN database changes occurred by entering the **show vlan** command from privileged EXEC mode.

Examples This example shows how to implement the proposed new VLAN database and to recognize it as the current database:

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

Related Commands

- abort** (refer to Cisco IOS documentation)
- exit** (refer to Cisco IOS documentation)
- reset**
- show vlan**
- shutdown vlan** (refer to Cisco IOS documentation)
- vtp (global configuration mode)**

arp access-list

To define an ARP access list or add clauses at the end of a predefined list, use the **arp access-list** command.

arp access-list *name*

Syntax Description	<i>name</i> Specifies the access control list name.
---------------------------	---

Defaults	None
-----------------	------

Command Modes	Configuration
----------------------	---------------

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples The following example shows how to define an ARP access list named static-hosts:

```
Switch(config)# arp access-list static-hosts
Switch(config)#
```

Related Commands	deny ip arp inspection filter vlan permit
-------------------------	---

attach module

To remotely connect to a specific module, use the **attach module** configuration command.

attach module *mod*

Syntax Description	<i>mod</i> Target module for the command.
---------------------------	---

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.1(19)EW	This command was first introduced.

Usage Guidelines	<p>This command applies only to the Access Gateway Module on Catalyst 4500 series switches.</p> <p>The valid values for <i>mod</i> depend on the chassis used. For example, if you have a Catalyst 4006 chassis, valid values for the module are from 2 to 6. If you have a 4507R chassis, valid values are from 3 to 7.</p> <p>When you execute the attach module <i>mod</i> command, the prompt changes to Gateway#.</p> <p>This command is identical in the resulting action to the session module <i>mod</i> and the remote login module <i>mod</i> commands.</p>
-------------------------	--

Examples	This example shows how to remotely log in to an Access Gateway Module:
-----------------	--

```
Switch# attach module 5
Attaching console to module 5
Type 'exit' at the remote prompt to end the session

Gateway>
```

Related Commands	remote login module session module
-------------------------	---

auto qos voip

To automatically configure quality of service (auto-QoS) for voice over IP (VoIP) within a QoS domain, use the **auto qos voip** interface configuration command. Use the **no** form of this command to change the auto-QoS configuration settings to the standard QoS defaults.

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

no auto qos voip { **cisco-phone** | **trust** }

Syntax Description

cisco-phone	Connects the interface to a Cisco IP phone and automatically configures QoS for VoIP. The CoS labels of incoming packets are trusted only when the telephone is detected.
trust	Connects the interface to a trusted switch or router and automatically configures QoS for VoIP. The CoS and DSCP labels of incoming packets are trusted.

Defaults

Auto-QoS is disabled on all interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 the edge devices that can classify incoming traffic for QoS.

Use the **cisco-phone** keyword on ports at the edge of the network that are connected to Cisco IP phones. The switch detects the telephone through the Cisco Discovery Protocol (CDP) and trusts the CoS labels in packets received from the telephone.

Use the **trust** keyword on ports connected to the interior of the network. Because it is assumed that traffic has already been classified by other edge devices, the CoS/DSCP labels in these packets are trusted.

When you enable the auto-QoS feature on the specified interface, these actions automatically occur:

- QoS is globally enabled (**qos** global configuration command).
- DBL is enabled globally (**qos dbl** global configuration command).
- When you enter the **auto qos voip cisco-phone** interface configuration command, the trusted boundary feature is enabled. It 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 specific interface is set to trust the CoS label received in the packet because some old phones do not mark DSCP. When a Cisco IP phone is absent, the ingress classification is set to not trust the CoS label in the packet.

- When you enter the **auto qos voip trust** interface configuration command, the ingress classification on the specified interface is set to trust the CoS label received in the packet if the specified interface is configured as Layer 2 (and is set to trust DSCP if the interface is configured as Layer 3).

You can enable auto-QoS on static, dynamic-access, voice VLAN access, and trunk ports.

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. Use the **debug auto qos** privileged EXEC command to enable auto-QoS debugging.

To disable auto-QoS on an interface, use the **no auto qos voip** interface configuration command. When you enter this command, the switch enables standard QoS and changes the auto-QoS settings to the standard QoS default settings for that interface. This action will not change any global configuration performed by auto-QoS; the global configuration remains the same.

Examples

This example shows how to enable auto-QoS and to trust the CoS and DSCP labels received in incoming packets when the switch or router connected to Gigabit Ethernet interface 1/1 is a trusted device:

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

This example shows how to enable auto-QoS and to trust the CoS labels received in incoming packets when the device connected to Fast Ethernet interface 2/1 is detected as a Cisco IP phone:

```
Switch(config)# interface fastethernet2/1
Switch(config-if)# auto qos voip cisco-phone
```

This example shows how to display the QoS configuration that is automatically generated when auto-QoS is enabled:

```
Switch# debug auto qos
AutoQoS debugging is on
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos voip trust
Switch(config-if)#
00:00:56:qos
00:00:57:qos map cos 3 to dscp 26
00:00:57:qos map cos 5 to dscp 46
00:00:58:qos map dscp 32 to tx-queue 1
00:00:58:qos dbl
00:01:00:policy-map autoqos-voip-policy
00:01:00: class class-default
00:01:00: dbl
00:01:00:interface GigabitEthernet1/1
00:01:00: qos trust cos
00:01:00: tx-queue 3
00:01:00: priority high
00:01:00: shape percent 33
00:01:00: service-policy output autoqos-voip-policy
Switchconfig-if)# interface gigabitethernet1/1
Switch(config-if)# auto qos voip cisco-phone
Switch(config-if)#
00:00:55:qos
00:00:56:qos map cos 3 to dscp 26
00:00:57:qos map cos 5 to dscp 46
00:00:58:qos map dscp 32 to tx-queue 1
00:00:58:qos dbl
00:00:59:policy-map autoqos-voip-policy
00:00:59: class class-default
```

■ auto qos voip

```
00:00:59: dbl
00:00:59:interface GigabitEthernet1/1
00:00:59: qos trust device cisco-phone
00:00:59: qos trust cos
00:00:59: tx-queue 3
00:00:59: priority high
00:00:59: shape percent 33
00:00:59: bandwidth percent 33
00:00:59: service-policy output autoqos-voip-policy
```

You can verify your settings by entering the **show auto qos interface** command.

Related Commands

debug auto qos (refer to Cisco IOS documentation)

qos map cos

qos trust

show auto qos

show qos

show qos interface

show qos maps

auto-sync

To enable automatic synchronization of the configuration files in NVRAM, use the **auto-sync** command. To disable automatic synchronization, use the **no** form of this command.

auto-sync { **startup-config** | **config-register** | **bootvar** | **standard** }

no auto-sync { **startup-config** | **config-register** | **bootvar** | **standard** }

Syntax Description		
	startup-config	Specifies automatic synchronization of the startup configuration.
	config-register	Specifies automatic synchronization of the configuration register configuration.
	bootvar	Specifies automatic synchronization of the BOOTVAR configuration.
	standard	Specifies automatic synchronization of the startup configuration, BOOTVAR, and configuration registers.

Defaults Standard automatic synchronization of all configuration files

Command Modes Redundancy main-cpu

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch (Catalyst4507R only).

Usage Guidelines If you enter the **no auto-sync standard** command, no automatic synchronizations occur.

Examples This example shows how (from the default configuration) to enable automatic synchronization of the configuration register in the main CPU:

```
Switch# config terminal
Switch (config)# redundancy
Switch (config-r)# main-cpu
Switch (config-r-mc)# no auto-sync standard
Switch (config-r-mc)# auto-sync configure-register
Switch (config-r-mc)#
```

Related Commands [redundancy](#)

channel-group

To assign and configure an EtherChannel interface to an EtherChannel group, use the **channel-group** command. To remove a channel group configuration from an interface, use the **no** form of this command.

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

no channel-group

Syntax Description		
number	Specifies the channel group number; valid values are from 1 to 64.	
mode	Specifies the EtherChannel mode of the interface.	
active	Enables LACP unconditionally.	
on	Forces the port to channel without PAgP.	
auto	Places a port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not initiate PAgP packet negotiation.	
non-silent	(Optional) Used with the auto or desirable mode when traffic is expected from the other device.	
passive	Enables LACP only if an LACP device is detected.	
desirable	Places a port into an active negotiating state, in which the port initiates negotiations with other ports by sending PAgP packets.	

Defaults No channel groups are assigned.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(13)EW	Support for LACP was added.

Usage Guidelines You do not have to create a port channel interface before assigning a physical interface to a channel group. If a port channel interface has not been created, it is automatically created when the first physical interface for the channel group is created.

If a specific channel number is used for the PAgP-enabled interfaces of a channel group, that same channel number cannot be used for configuring a channel that has LACP-enabled interfaces or vice versa.

You can also create port channels by entering the **interface port-channel** command. This will create a Layer 3 port channel. To change the Layer 3 port channel into a Layer 2 port channel, use the **switchport** command before you assign physical interfaces to the channel group. A port channel cannot be changed from Layer 3 to Layer 2 or vice versa when it contains member ports.

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

Any configuration or attribute changes you make to the port-channel interface are propagated to all interfaces within the same channel group as the port channel (for example, configuration changes are also propagated to the physical interfaces that are not part of the port channel, but are part of the channel group).

You can create in **on** mode a usable EtherChannel by connecting two port groups together.

**Caution**

Do not enable Layer3 addresses on the physical EtherChannel interfaces. Do not assign bridge groups on the physical EtherChannel interfaces because it creates loops.

Examples

This example shows how to add Gigabit Ethernet interface 1/1 to the EtherChannel group specified by port channel 45:

```
Switch(config-if)# channel-group 45 mode on  
Creating a port-channel interface Port-channel45  
Switch(config-if)#
```

Related Commands

interface port-channel
show interfaces port-channel (refer to Cisco IOS documentation)

channel-protocol

To enable LACP or PAgP on an interface, use the **channel-protocol** command. To disable the protocols, use the **no** form of this command.

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

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

Syntax Description

lACP	Enables LACP to manage channeling.
pagp	Enables PAgP to manage channeling.

Defaults

PAgP

Command Modes

Interface configuration

Command History

Release	Modification
12.1(13)EW	Support for this command was introduced on the Catalyst4500 series switches.

Usage Guidelines

This command is not supported on systems configured with a Supervisor Engine 1.

You can also select the protocol using the **channel-group** command.

If the interface belongs to a channel, the **no** form of this command is rejected.

All ports in an EtherChannel must use the same protocol; you cannot run two protocols on one module.

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

You can manually configure a switch with PAgP on one side and LACP on the other side in the **on** mode.

You can change the protocol at any time, but this change causes all existing EtherChannels to reset to the default channel mode for the new protocol. You can use the **channel-protocol** command to restrict anyone from selecting a mode that is not applicable to the selected protocol.

Configure all ports in an EtherChannel to operate at the same speed and duplex mode (full duplex only for LACP mode).

For a complete list of guidelines, refer to the “Configuring EtherChannel” section of the *Catalyst4500 Series Switch CiscoIOS Software Configuration Guide*.

Examples

This example shows how to select LACP to manage channeling on the interface:

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


Related Commands

[channel-group](#)
[show etherchannel](#)

class-map

To access the QoS class map configuration mode to configure QoS class maps, use the **class-map** command. To delete a class map, use the **no** form of this command.

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

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

Syntax Description

match-all	(Optional) Specifies that all match criteria in the class map must be matched.
match-any	(Optional) Specifies that one or more match criteria must match.
<i>name</i>	Name of the class map.

Defaults

Match all criteria.

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The variables *name* and *acl_name* are case sensitive.

Use the **class-map** command and its subcommands on individual interfaces to define packet classification, marking, aggregate, and flow policing as part of a globally named service policy.

These commands are available in QoS class map configuration mode:

- **exit**—Exits you from QoS class map configuration mode.
- **no**—Removes a match statement from a class map.
- **match**—Configures classification criteria.

These optional subcommands are also available:

- **access-group** {*acl_index* | **name** *acl_name*}
- **ip** {**dscp** | **precedence**} *value1 value2... value8*
- **any**

The following subcommands appear in the CLI help, but they are not supported on LAN interfaces:

- **input-interface** {*interface interface_number* | **null** *number* | **vlan** *vlan_id*}
- **protocol** *linktype*
- **destination-address** **mac** *mac_address*
- **source-address** **mac** *mac_address*
- **qos-group**

- **mpls**
- **no**

After you have configured the class map name and are in class map configuration mode, you can enter the **match** subcommands. The syntax for these subcommands is as follows:

```
match {[access-group {acl_index | name acl_name}] | [ip {dscp | precedence} value1 value2...
value8]}
```

See [Table2-1](#) for a syntax description of the **match** subcommands.

Table2-1 Syntax Description for the match Command

Optional Subcommand	Description
access-group <i>acl_index</i> <i>acl_name</i>	Specifies the access list index or access list names; valid access list index values are from 1 to 2699.
access-group <i>acl_name</i>	Specifies the named access list.
ip dscp <i>value1 value2</i> ... <i>value8</i>	Specifies IP DSCP values to match; valid values are from 0 to 63. Enter up to eight DSCP values separated by white spaces.
ip precedence <i>value1</i> <i>value2 ... value8</i>	Specifies IP precedence values to match; valid values are from 0 to 7. Enter up to eight precedence values separated by white spaces.

Examples

This example shows how to access the **class-map** commands and subcommands and to configure a class map named **ipp5** and enter a match statement for ip precedence 5:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map ipp5
Switch(config-cmap)# match ip precedence 5
Switch(config-cmap)#
```

This example shows how to configure the class map to match an already configured access list:

```
Switch(config-cmap)# match access-group IPacl1
Switch(config-cmap)#
```

Related Commands

[policy-map](#)
[service-policy](#)
[show class-map](#)
[show policy-map](#)
[show policy-map interface](#)

clear counters

To clear interface counters, use the **clear counters** command.

```
clear counters [{FastEthernet interface_number} | {GigabitEthernet interface_number} |
  {null interface_number} | {port-channel number} | {vlan vlan_id}]
```

Syntax Description

FastEthernet <i>interface_number</i>	(Optional) Specifies the Fast Ethernet interface; valid values are from 1 to 9.
GigabitEthernet <i>interface_number</i>	(Optional) Specifies the Gigabit Ethernet interface; valid values are from 1 to 9.
null <i>interface_number</i>	(Optional) Specifies the null interface; the valid value is 0.
port-channel <i>number</i>	(Optional) Specifies the channel interface; valid values are from 1 to 64.
vlan <i>vlan_id</i>	(Optional) Specifies the VLAN; valid values are from 1 to 4096.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Support for extended VLAN addresses was added.

Usage Guidelines

This command clears all the current interface counters from all interfaces unless you specify an interface.



Note

This command does not clear counters retrieved using SNMP, but only those seen when you enter the **show interface counters** command.

Examples

This example shows how to clear all interface counters:

```
Switch# clear counters
Clear "show interface" counters on all interfaces [confirm] y
Switch#
```

This example shows how to clear counters on a specific interface:

```
Switch# clear counters vlan 200
Clear "show interface" counters on this interface [confirm]
Switch#
```

Related Commands **show interface counters** (refer to Cisco IOS documentation)

clear hw-module slot password

To clear the password on an intelligent line module, use the **clear hw-module slot password** command:

```
clear hw-module slot slot_num password
```

Syntax Description	<i>slot_num</i> (Optional) Specifies a slot on a line module.
---------------------------	---

Defaults	The password is not cleared.
-----------------	------------------------------

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

Command History	Release	Modification
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	You only need to change the password once unless the password is reset.
-------------------------	---

Examples	This example shows how to clear the password from slot 5 on a line module:
-----------------	--

```
Switch# clear hw-module slot 5 password
Switch#
```

Related Commands	hw-module power
-------------------------	---------------------------------

clear interface gigabitethernet

To clear the hardware logic from a Gigabit Ethernet IEEE 802.3z interface, use the **clear interface .gigabitethernet** command.

clear interface gigabitethernet *slot/port*

Syntax Description	<i>slot/port</i> Number of the slot and port.				
Defaults	This command has no default settings.				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(8a)EW</td> <td>Support for this command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Release	Modification				
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.				
Examples	<p>This example shows how to clear the hardware logic from a Gigabit Ethernet IEEE 802.3z interface:</p> <pre>Switch# clear interface gigabitethernet 1/1 Switch#</pre>				
Related Commands	show interfaces status				

clear interface vlan

To clear the hardware logic from a VLAN, use the **clear interface vlan** command.

clear interface vlan *number*

Syntax Description	<i>number</i> Number of the VLAN interface; valid values are from 1 to 4094.
---------------------------	--

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Support for extended VLAN addresses added.	

Examples	This example shows how to clear the hardware logic from a specific VLAN:
-----------------	--

```
Switch# clear interface vlan 5
Switch#
```

Related Commands	show interfaces status
-------------------------	--

clear ip access-template

To clear statistical information in access lists, use the **clear ip access-template** command.

clear ip access-template *access-list*

Syntax Description	<i>access-list</i> Number of the access list; valid values are from 100 to 199 for an IP extended access list, and from 2000 to 2699 for an expanded range IP extended access list.
---------------------------	---

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples	This example shows how to clear statistical information for an access list:
-----------------	---

```
Switch# clear ip access-template 201
Switch#
```

clear ip arp inspection log

To clear the status of the log buffer, use the **clear ip arp inspection log command**.

clear ip arp inspection log

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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

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

Related Commands

- [arp access-list](#)
- [show ip arp inspection log](#)

clear ip arp inspection statistics

To clear the dynamic ARP inspection statistics, use the **clear ip arp inspection statistics** command.

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

Syntax Description	vlan <i>vlan-range</i> (Optional) Specifies the VLAN range.				
Defaults	This command has no default settings.				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(19)EW</td> <td>Support for this command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Release	Modification				
12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.				

Examples

This example shows to clear the DAI statistics from VLAN 1:

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

Vlan      Forwarded      Dropped      DHCP Drops      ACL Drops
----      -
1         0              0            0              0

Vlan      DHCP Permits   ACL Permits   Source MAC Failures
----      -
1         0              0              0

Vlan      Dest MAC Failures  IP Validation Failures
----      -
1         0                  0

Switch#
```

Related Commands

[arp access-list](#)
[clear ip arp inspection log](#)
[show ip arp inspection](#)

clear ip dhcp snooping database

To clear the DHCP binding database, use the **clear ip dhcp snooping database** command.

clear ip dhcp snooping database

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to clear the DHCP binding database:

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

Related Commands

- [ip dhcp snooping](#)
- [ip dhcp snooping binding interface](#) (refer to Cisco IOS documentation)
- [ip dhcp snooping information option](#)
- [ip dhcp snooping trust](#)
- [ip dhcp snooping vlan](#)
- [show ip dhcp snooping](#)
- [show ip dhcp snooping binding](#)

clear ip dhcp snooping database statistics

To clear DHCP binding database statistics, use the **clear ip dhcp snooping database statistics** command.

clear ip dhcp snooping database statistics

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to clear the DHCP binding database:

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

Related Commands

- [ip dhcp snooping](#)
- [ip dhcp snooping binding](#)
- [ip dhcp snooping information option](#)
- [ip dhcp snooping trust](#)
- [ip dhcp snooping vlan](#)
- [show ip dhcp snooping](#)
- [show ip dhcp snooping binding](#)

clear ip igmp group

To delete IGMP group cache entries, use the **clear ip igmp group** command.

```
clear ip igmp group [{fastethernet slot/port} | {GigabitEthernet slot/port} | {host_name |
group_address} {Loopback interface_number} | {null interface_number} |
{port-channel number} | {vlan vlan_id}]
```

Syntax Description		
fastethernet	(Optional)	Specifies the Fast Ethernet interface.
<i>slot/port</i>	(Optional)	Number of the slot and port.
GigabitEthernet	(Optional)	Specifies the Gigabit Ethernet interface.
<i>host_name</i>	(Optional)	Hostname, as defined in the DNS hosts table or with the ip host command.
<i>group_address</i>	(Optional)	Address of the multicast group in four-part, dotted notation.
Loopback <i>interface_number</i>	(Optional)	Specifies the loopback interface; valid values are from 0 to 2,147,483,647.
null <i>interface_number</i>	(Optional)	Specifies the null interface; the valid value is 0.
port-channel <i>number</i>	(Optional)	Specifies the channel interface; valid values are from 1 to 64.
vlan <i>vlan_id</i>	(Optional)	Specifies the VLAN; valid values are from 1 to 4094.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines The IGMP cache contains a list of the multicast groups of which hosts on the directly connected LAN are members.

To delete all entries from the IGMP cache, enter the **clear ip igmp group** command with no arguments.

Examples This example shows how to clear entries for a specific group from the IGMP cache:

```
Switch# clear ip igmp group 224.0.255.1
Switch#
```

This example shows how to clear IGMP group cache entries from a specific interface:

```
Switch# clear ip igmp group gigabitethernet 2/2
Switch#
```

Related Commands

ip host (refer to Cisco IOS documentation)

show ip igmp groups (refer to Cisco IOS documentation)

show ip igmp interface

clear ip igmp snooping membership

To clear the explicit host tracking database, use the **clear ip igmp snooping membership** command.

clear ip igmp snooping membership [**vlan** *vlan_id*]

Syntax Description	vlan <i>vlan_id</i> (Optional) Specifies a VLAN; valid values are from 1 to 1001 and from 1006 to 4094.
---------------------------	--

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	By default, the explicit host tracking database maintains a maximum of 1 KB entries. After you reach this limit, no additional entries can be created in the database. To create more entries, you will need to delete the database with the clear ip igmp snooping statistics vlan command.
-------------------------	---

Examples	This example shows how to display IGMP snooping statistics for VLAN 25:
-----------------	---

```
Switch# clear ip igmp snooping membership vlan 25
Switch#
```

Related Commands	ip igmp snooping vlan explicit-tracking show ip igmp snooping membership
-------------------------	---

clear ip mfib counters

To clear global MFIB counters and counters for all active MFIB routes, use the **clear ip mfib counters** command.

clear ip mfib counters

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to clear all the active MFIB routes and global counters:

```
Switch# clear ip mfib counters
Switch#
```

Related Commands [show ip mfib](#)

clear ip mfib fastdrop

To clear all MFIB fast drop entries, use the **clear ip mfib fastdrop** command.

clear ip mfib fastdrop

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines If new fast-dropped packets arrive, new fast drop entries are created.

Examples This example shows how to clear all fast drop entries:

```
Switch# clear ip mfib fastdrop
Switch#
```

Related Commands [ip mfib fastdrop](#)
[show ip mfib fastdrop](#)

clear lacp counters

To clear statistics for all interfaces belonging to a specific channel group, use the **clear lacp counters** command.

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

Syntax Description	<i>channel-group</i> (Optional) Channel group number; valid values are from 1 to 64.
---------------------------	--

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst4500 series switches.

Usage Guidelines	<p>This command is not supported on systems configured with a Supervisor Engine 1.</p> <p>If you do not specify a channel group, all channel groups are cleared.</p> <p>If you enter this command for a channel group that contains members in PAgP mode, the command is ignored.</p>
-------------------------	---

Examples	This example shows how to clear the statistics for a specific group:
-----------------	--

```
Switch# clear lacp 1 counters
Switch#
```

Related Commands	show lacp
-------------------------	---------------------------

clear mac-address-table dynamic

To clear dynamic address entries from the Layer 2 MAC address table, use the **clear mac-address-table dynamic** command.

```
clear mac-address-table dynamic [{address mac_addr} | {interface interface}] [vlan vlan_id]
```

Syntax Description	address <i>mac_addr</i> (Optional) Specifies the MAC address.
	interface <i>interface</i> (Optional) Specifies the interface and clear the entries associated with it; valid values are FastEthernet and GigabitEthernet .
	vlan <i>vlan_id</i> (Optional) Specifies the VLANs; valid values are from 1 to 4094.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended VLAN addresses added.

Usage Guidelines Enter the **clear mac-address-table dynamic** command with no arguments to remove all dynamic entries from the table.

Examples This example shows how to clear all dynamic Layer 2 entries for a specific interface (gi1/1):

```
Switch# clear mac-address-table dynamic interface gi1/1
Switch#
```

Related Commands

- [mac-address-table aging-time](#)
- [main-cpu](#)
- [show mac-address-table address](#)

clear pagp

To clear port channel information, use the **clear pagp** command.

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

Syntax Description	
<i>group-number</i>	Channel group number; valid values are from 1 to 64.
counters	Clears traffic filters.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to clear port channel information for a specific group:

```
Switch# clear pagp 32
Switch#
```

This example shows how to clear all port channel traffic filters:

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

Related Commands [show pagp](#)

clear port-security

To delete from the MAC address table all secure addresses, all configured secure addresses, or a specific dynamic or sticky secure address on an interface, use the **clear port-security** command.

clear port-security { **all** | **dynamic** } [**address** *mac-addr* [**vlan** *vlan-id*]] | [**interface** *interface-id*]

Syntax Description		
all		Deletes all secure MAC addresses.
dynamic		Deletes all dynamic secure MAC addresses.
address <i>mac-addr</i>	(Optional)	Deletes the specified secure MAC address.
vlan <i>vlan-id</i>	(Optional)	Deletes the specified secure MAC address from the specified VLAN.
interface <i>interface-id</i>	(Optional)	Deletes secure MAC addresses on the specified physical port or port channel.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Usage Guidelines If you enter the **clear port-security all** command, the switch removes all secure MAC addresses from the MAC address table.

If you enter the **clear port-security dynamic interface interface-id** command, the switch removes all dynamic secure MAC addresses on an interface from the MAC address table.

Command History	Release	Modification
	12.2(18)EW	This command was first introduced on the Catalyst 4500 series switch.

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

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

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

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

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

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

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

Related Commands [show port-security](#)
[switchport port-security](#)

clear qos

To clear global and per-interface aggregate QoS counters, use the **clear qos** command.

```
clear qos [aggregate-policer name] | interface { fastethernet | GigabitEthernet }
{ slot/interface } | vlan { vlan_num } | port-channel { number }
```

Syntax Description

aggregate-policer <i>name</i>	(Optional) Specifies an aggregate policer.
interface	(Optional) Specifies an interface.
fastethernet	(Optional) Specifies the Fast Ethernet 802.3 interface.
GigabitEthernet	(Optional) Specifies the Gigabit Ethernet 802.3z interface.
<i>slot/interface</i>	(Optional) Number of the slot and interface.
vlan <i>vlan_num</i>	(Optional) Specifies a VLAN.
port-channel <i>number</i>	(Optional) Specifies the channel interface; valid values are from 1 to 64.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines



Note

When you enter the **clear qos** command, the way that the counters work is affected and traffic that is normally restricted could be forwarded for a short period of time.

The **clear qos** command resets the interface QoS policy counters. If no interface is specified, the **clear qos** command resets the QoS policy counters for all interfaces.

Examples

This example shows how to clear global and per-interface aggregate QoS counters for all protocols:

```
Switch# clear qos
Switch#
```

This example shows how to clear specific protocol aggregate QoS counters for all interfaces:

```
Switch# clear qos aggregate-policer
Switch#
```

Related Commands

[show qos](#)

clear vlan counters

To clear the software-cached counter values to start from zero again for a specified VLAN or all existing VLANs, use the **clear vlan counters** command.

clear vlan [*vlan-id*] **counters**

Syntax Description	<i>vlan-id</i> (Optional) VLAN number; see “Usage Guidelines” for valid values.
---------------------------	---

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst4500 series switches.

Usage Guidelines	If you do not specify a <i>vlan-id</i> value; the software-cached counter values for all existing VLANs are cleared.
-------------------------	--

Examples	This example shows how to clear the software-cached counter values for a specific VLAN:
-----------------	---

```
Switch# clear vlan 10 counters
Clear "show vlan" counters on this vlan [confirm]
Switch#
```

Related Commands	show vlan counters
-------------------------	------------------------------------

clear vmps statistics

To clear VMPS statistics, use the **clear vmps statistics** command.

clear vmps statistics

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst4500 series switches.

Examples This example shows how to clear VMPS statistics:

```
Switch# clear vmps statistics
Switch#
```

Related Commands [show vmps](#)
[vmps reconfirm \(privileged EXEC\)](#)

debug adjacency

To display adjacency debugging information, use the **debug adjacency** command. To disable debugging output, use the **no** form of this command.

debug adjacency [ipc]

no debug adjacency

Syntax Description	ipc (Optional) Displays IPC entries in the adjacency database.
---------------------------	---

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples	This example shows how to display information in the adjacency database:
-----------------	--

```
Switch# debug adjacency
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
<... output truncated...>
Switch#
```

Related Commands	undebug adjacency (same as no debug adjacency)
-------------------------	---

debug backup

To debug backup events, use the **debug backup** command. To disable debugging output, use the **no** form of this command.

debug backup

no debug backup

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to debug backup events:

```
Switch# debug backup
Backup events debugging is on
Switch#
```

Related Commands **undebug backup** (same as **no debug backup**)

debug condition interface

To limit debugging output of interface-related activities, use the **debug condition interface** command. To disable debugging output, use the **no** form of this command.

```
debug condition interface { fastethernet slot/port | GigabitEthernet slot/port |
null interface_num | port-channel interface-num | vlan vlan_id }
```

```
no debug condition interface { fastethernet slot/port | GigabitEthernet slot/port | null
interface_num | port-channel interface-num | vlan vlan_id }
```

Syntax Description		
fastethernet		Limits debugging to Fast Ethernet interfaces.
<i>slot/port</i>		Number of the slot and port.
GigabitEthernet		Limits debugging to Gigabit Ethernet interfaces.
null <i>interface-num</i>		Limits debugging to null interfaces; the valid value is 0.
port-channel <i>interface-num</i>		Limits debugging to port-channel interfaces; valid values are from 1 to 64.
vlan <i>vlan_id</i>		Specifies the VLAN interface number; valid values are from 1 to 4094.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended VLAN addresses added.

Examples This example shows how to limit debugging output to VLAN interface 1:

```
Switch# debug condition interface vlan 1
Condition 2 set
Switch#
```

Related Commands [debug interface](#)
undebug condition interface (same as **no debug condition interface**)

debug condition standby

To limit debugging output for standby state changes, use the **debug condition standby** command. To disable debugging output, use the **no** form of this command.

```
debug condition standby {fastethernet slot/port | GigabitEthernet slot/port |
port-channel interface-num | vlan vlan_id group-number}
```

```
no debug condition standby {fastethernet slot/port | GigabitEthernet slot/port |
port-channel interface-num | vlan vlan_id group-number}
```

Syntax Description		
fastethernet		Limits debugging to Fast Ethernet interfaces.
<i>slot/port</i>		Number of the slot and port.
GigabitEthernet		Limits debugging to Gigabit Ethernet interfaces.
port-channel <i>interface_num</i>		Limits debugging output to port-channel interfaces; valid values are from 1 to 64.
vlan <i>vlan_id</i>		Limits debugging of a condition on a VLAN interface; valid values are from 1 to 4094.
<i>group-number</i>		VLAN group number; valid values are from 0 to 255.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended VLAN addresses added.

Usage Guidelines If you attempt to remove the only condition set, you will be prompted with a message asking if you want to abort the removal operation. You can enter **n** to abort the removal or **y** to proceed with the removal. If you remove the only condition set, an excessive number of debugging messages might occur.

Examples This example shows how to limit the debugging output to group 0 in VLAN 1:

```
Switch# debug condition standby vlan 1 0
Condition 3 set
Switch#
```

This example shows the display if you try to turn off the last standby debug condition:

```
Switch# no debug condition standby vlan 1 0
This condition is the last standby condition set.
Removing all conditions may cause a flood of debugging
messages to result, unless specific debugging flags
```

debug condition standby

are first removed.

```
Proceed with removal? [yes/no]: n
% Operation aborted
Switch#
```

Related Commands **undebg condition standby** (same as **no debug condition standby**)

debug condition vlan

To limit VLAN debugging output for a specific VLAN, use the **debug condition vlan** command. To disable debugging output, use the **no** form of this command.

```
debug condition vlan {vlan_id}
```

```
no debug condition vlan {vlan_id}
```

Syntax Description	<i>vlan_id</i> Number of the VLAN; valid values are from 1 to 4096.
---------------------------	---

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended VLAN addresses added.

Usage Guidelines	If you attempt to remove the only VLAN condition set, you will be prompted with a message asking if you want to abort the removal operation. You can enter n to abort the removal or y to proceed with the removal. If you remove the only condition set, it could result in the display of an excessive number of messages.
-------------------------	--

Examples	This example shows how to limit debugging output to VLAN 1:
-----------------	---

```
Switch# debug condition vlan 1
Condition 4 set
Switch#
```

This example shows the message that is displayed when you attempt to disable the last VLAN debug condition:

```
Switch# no debug condition vlan 1
This condition is the last vlan condition set.
Removing all conditions may cause a flood of debugging
messages to result, unless specific debugging flags
are first removed.

Proceed with removal? [yes/no]: n
% Operation aborted
Switch#
```

Related Commands	undebug condition vlan (same as no debug condition vlan)
-------------------------	---

debug dot1x

To enable debugging for the 802.1x feature, use the **debug dot1x** command. Use the **no** form of this command to disable debugging output.

debug dot1x {**all** | **errors** | **events** | **packets** | **registry** | **state-machine** }

no debug dot1x {**all** | **errors** | **events** | **packets** | **registry** | **state-machine** }

Syntax Description		
	all	Enables debugging of all conditions.
	errors	Enables debugging of print statements guarded by the dot1x error flag.
	events	Enables debugging of print statements guarded by the dot1x events flag.
	packets	All incoming dot1x packets are printed with packet and interface information.
	registry	Enables debugging of print statements guarded by the dot1x registry flag.
	state-machine	Enables debugging of print statements guarded by the dot1x registry flag.

Defaults Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Related Commands [show dot1x](#)
undebug dot1x (same as **no debug dot1x**)

debug etherchnl

To debug EtherChannel, use the **debug etherchnl** command. To disable debugging output, use the **no** form of this command.

debug etherchnl [**all** | **detail** | **error** | **event** | **idb** | **linecard**]

no debug etherchnl

Syntax Description	
all	(Optional) Displays all EtherChannel debug messages.
detail	(Optional) Displays detailed EtherChannel debug messages.
error	(Optional) Displays EtherChannel error messages.
event	(Optional) Debugs major EtherChannel event messages.
idb	(Optional) Debugs PAgP IDB messages.
linecard	(Optional) Debugs SCP messages to the module.

Defaults

The default settings are as follows:

- Debug is disabled.
- All messages are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

If you do not specify a keyword, all debug messages are displayed.

Examples

This example shows how to display all EtherChannel debug messages:

```
Switch# debug etherchnl
PAgP Shim/FEC debugging is on
22:46:30:FEC:returning agport Po15 for port (Fa2/1)
22:46:31:FEC:returning agport Po15 for port (Fa4/14)
22:46:33:FEC:comparing GC values of Fa2/25 Fa2/15 flag = 1 1
22:46:33:FEC:port_attrib:Fa2/25 Fa2/15 same
22:46:33:FEC:EC - attrib incompatable for Fa2/25; duplex of Fa2/25 is half, Fa2/15 is full
22:46:33:FEC:pagp_switch_choose_unique:Fa2/25, port Fa2/15 in agport Po3 is incompatable
Switch#
```

This example shows how to display EtherChannel IDB debug messages:

```
Switch# debug etherchnl idb
Agport idb related debugging is on
Switch#
```

■ debug etherchnl

This example shows how to disable debugging:

```
Switch# no debug etherchnl  
Switch#
```

Related Commands **undebug etherchnl** (same as **no debug etherchnl**)

debug interface

To abbreviate entry of the **debug condition interface** command, use the **debug interface** command. To disable debugging output, use the **no** form of this command.

```
debug interface { FastEthernet slot/port | GigabitEthernet slot/port | null |
port-channel interface-num | vlan vlan_id}
```

```
no debug interface { FastEthernet slot/port | GigabitEthernet slot/port | null |
port-channel interface-num | vlan vlan_id}
```

Syntax Description	FastEthernet	Limits debugging to Fast Ethernet interfaces.
	<i>slot/port</i>	Number of the slot and port.
	GigabitEthernet	Limits debugging to Gigabit Ethernet interfaces.
	null	Limits debugging to null interfaces; the only valid value is 0.
	port-channel	<i>interface-num</i>
		Limits debugging to port-channel interfaces; valid values are from 1 to 64.
	vlan	<i>vlan_id</i>
		Specifies the VLAN interface number; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Support for extended VLAN addresses added.

Examples

This example shows how to limit debugging to interface VLAN 1:

```
Switch# debug interface vlan 1
Condition 1 set
Switch#
```

Related Commands

debug condition interface
undebug interface (same as **no debug interface**)

debug ipc

To debug IPC activity, use the **debug ipc** command. To disable debugging output, use the **no** form of this command.

debug ipc { **all** | **errors** | **events** | **headers** | **packets** | **ports** | **seats** }

no debug ipc { **all** | **errors** | **events** | **headers** | **packets** | **ports** | **seats** }

Syntax Description

all	Enables all IPC debugging.
errors	Enables IPC error debugging.
events	Enables IPC event debugging.
headers	Enables IPC header debugging.
packets	Enables IPC packet debugging.
ports	Enables debugging of the creation and deletion of ports.
seats	Enables debugging of the creation and deletion of nodes.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

This example shows how to enable debugging of IPC events:

```
Switch# debug ipc events
Special Events debugging is on
Switch#
```

Related Commands

undebug ipc (same as **no debug ipc**)

debug ip dhcp snooping event

To debug DHCP snooping events, use the **debug ip dhcp snooping event** command. To disable debugging output, use the **no** form of this command.

debug ip dhcp snooping event

no debug ip dhcp snooping event

Syntax Description This command has no arguments or keywords.

Defaults Debugging of snooping event is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to enable debugging for DHCP snooping events:

```
Switch# debug ip dhcp snooping event
Switch#
```

This example shows how to disable debugging for DHCP snooping events:

```
Switch# no debug ip dhcp snooping event
Switch#
```

Related Commands [debug ip dhcp snooping packet](#)

debug ip dhcp snooping packet

To debug DHCP snooping messages, use the **debug ip dhcp snooping packet** command. To disable debugging output, use the **no** form of this command.

debug ip dhcp snooping packet

no debug ip dhcp snooping packet

Syntax Description This command has no arguments or keywords.

Defaults Debugging of snooping packet is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to enable debugging for DHCP snooping packets:

```
Switch# debug ip dhcp snooping packet
Switch#
```

This example shows how to disable debugging for DHCP snooping packets:

```
Switch# no debug ip dhcp snooping packet
Switch#
```

Related Commands [debug ip dhcp snooping event](#)

debug ip verify source packet

To debug IP source guard messages, use the **debug ip verify source packet** command. To disable debugging output, use the **no** form of this command.

debug ip verify source packet

no debug ip verify source packet

Syntax Description This command has no arguments or keywords.

Defaults Debugging of snooping security packets is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to enable debugging for IP source guard:

```
Switch# debug ip verify source packet
Switch#
```

This example shows how to disable debugging for IP source guard:

```
Switch# no debug ip verify source packet
Switch#
```

Related Commands

- [ip dhcp snooping](#)
- [ip dhcp snooping information option](#)
- [ip dhcp snooping limit rate](#)
- [ip dhcp snooping trust](#)
- [ip verify source vlan dhcp-snooping](#) (refer to Cisco IOS documentation)
- [show ip dhcp snooping](#)
- [show ip dhcp snooping binding](#)
- [show ip verify source](#) (refer to Cisco IOS documentation)

debug lacp

To debug LACP activity, use the **debug lacp** command. To disable debugging output, use the **no** form of this command.

debug lacp [**all** | **event** | **fsm** | **misc** | **packet**]

no debug lacp

Syntax Description

all	(Optional) Enables all LACP debugging.
event	(Optional) Enables debugging of LACP events.
fsm	(Optional) Enables debugging of the LACP finite state machine.
misc	(Optional) Enables miscellaneous LACP debugging.
packet	(Optional) Enables LACP packet debugging.

Defaults

Debugging of LACP activity is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

This command is supported by the supervisor engine only and can be entered only from the switch console.

Examples

This example shows how to enable LACP miscellaneous debugging:

```
Switch# debug lacp
Port Aggregation Protocol Miscellaneous debugging is on
Switch#
```

Related Commands

undebug pagp (same as **no debug pagp**)

debug monitor

To display monitoring activity, use the **debug monitor** command. To disable debugging output, use the **no** form of this command.

debug monitor { **all** | **errors** | **idb-update** | **list** | **notifications** | **platform** | **requests** }

no debug monitor { **all** | **errors** | **idb-update** | **list** | **notifications** | **platform** | **requests** }

Syntax Description		
all	Displays all SPAN debugging messages.	
errors	Displays SPAN error details.	
idb-update	Displays SPAN IDB update traces.	
list	Displays SPAN and VLAN list tracing.	
notifications	Displays SPAN notifications.	
platform	Displays SPAN platform tracing.	
requests	Displays SPAN requests.	

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to debug monitoring errors:

```
Switch# debug monitor errors
SPAN error detail debugging is on
Switch#
```

Related Commands **undebug monitor** (same as **no debug monitor**)

debug nvram

To debug NVRAM activity, use the **debug nvram** command. To disable debugging output, use the **no** form of this command.

debug nvram

no debug nvram

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to debug NVRAM:

```
Switch# debug nvram
NVRAM behavior debugging is on
Switch#
```

Related Commands **undebug nvram** (same as **no debug nvram**)

debug pagp

To debug PAgP activity, use the **debug pagp** command. To disable debugging output, use the **no** form of this command.

debug pagp [**all** | **event** | **fsm** | **misc** | **packet**]

no debug pagp

Syntax Description	
all	(Optional) Enables all PAgP debugging.
event	(Optional) Enables debugging of PAgP events.
fsm	(Optional) Enables debugging of the PAgP finite state machine.
misc	(Optional) Enables miscellaneous PAgP debugging.
packet	(Optional) Enables PAgP packet debugging.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines This command is supported by the supervisor engine only and can be entered only from the switch console.

Examples This example shows how to enable PAgP miscellaneous debugging:

```
Switch# debug pagp misc
Port Aggregation Protocol Miscellaneous debugging is on
Switch#
*Sep 30 10:13:03: SP: PAgP: pagp_h(Fa5/6) expired
*Sep 30 10:13:03: SP: PAgP: 135 bytes out Fa5/6
*Sep 30 10:13:03: SP: PAgP: Fa5/6 Transmitting information packet
*Sep 30 10:13:03: SP: PAgP: timer pagp_h(Fa5/6) started with interval 30000
<... output truncated...>
Switch#
```

Related Commands **undebug pagp** (same as **no debug pagp**)

debug platform packet protocol lacp

To debug LACP protocol packets, use the **debug platform packet protocol lacp** command. To disable debugging output, use the **no** form of this command.

debug platform packet protocol lacp [receive | transmit | vlan]

no debug platform packet protocol lacp [receive | transmit | vlan]

Syntax Description

receive	(Optional) Enables platform packet reception debugging functions.
transmit	(Optional) Enables platform packet transmission debugging functions.
vlan	(Optional) Enables platform packet VLAN debugging functions.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

This example shows how to enable all PM debugging:

```
Switch# debug platform packet protocol lacp
Switch#
```

Related Commands

undebug platform packet protocol lacp (same as **no debug platform packet protocol lacp**)

debug platform packet protocol pagp

To debug PAgP protocol packets, use the **debug platform packet protocol lacp** command. To disable debugging output, use the **no** form of this command.

debug platform packet protocol pagp [receive | transmit | vlan]

no debug platform packet protocol pagp [receive | transmit | vlan]

Syntax Description

receive	Enables platform packet reception debugging functions.
transmit	Enables platform packet transmission debugging functions.
vlan	Enables platform packet VLAN debugging functions.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

This example shows how to enable all PM debugging:

```
Switch# debug platform packet protocol pagp
Switch#
```

Related Commands

undebug platform packet protocol pagp (same as **no debug platform packet protocol pagp**)

debug pm

To debug port manager (PM) activity, use the **debug pm** command. To disable debugging output, use the **no** form of this command.

```
debug pm { all | card | cookies | etherchnl | messages | port | registry | scp | sm | span | split |
vlan | vp }
```

```
no debug pm { all | card | cookies | etherchnl | messages | port | registry | scp | sm | span | split |
vlan | vp }
```

Syntax Description

all	Displays all PM debugging messages.
card	Debugs module-related events.
cookies	Enables internal PM cookie validation.
etherchnl	Debugs EtherChannel-related events.
messages	Debugs PM messages.
port	Debugs port-related events.
registry	Debugs PM registry invocations.
scp	Debugs SCP module messaging.
sm	Debugs state machine-related events.
span	Debugs spanning tree-related events.
split	Debugs split-processor.
vlan	Debugs VLAN-related events.
vp	Debugs virtual port-related events.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

This example shows how to enable all PM debugging:

```
Switch# debug pm all
Switch#
```

Related Commands

undebug pm (same as **no debug pm**)

debug psecure

To debug port security, use the **debug psecure** command. To disable debugging output, use the **no** form of this command.

debug psecure

no debug psecure

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Release	Modification
12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to enable all PM debugging:

```
Switch# debug psecure
Switch#
```

Related Commands [switchport port-security](#)

debug redundancy

To debug supervisor redundancy, use the **debug redundancy** command. To disable debugging output, use the **no** form of this command.

debug redundancy { errors | fsm | kpa | msg | progression | status | timer }

no debug redundancy

Syntax Description

errors	Enables redundancy facility for error debugging.
fsm	Enables redundancy facility for FSM event debugging.
kpa	Enables redundancy facility for keepalive debugging.
msg	Enables redundancy facility for messaging event debugging.
progression	Enables redundancy facility for progression event debugging.
status	Enables redundancy facility for status event debugging.
timer	Enables redundancy facility for timer event debugging.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch (Catalyst 4507R only).

Examples

This example shows how to debug redundancy facility timer event debugging:

```
Switch# debug redundancy timer
Redundancy timer debugging is on
Switch#
```


debug smf updates

To debug software MAC filter (SMF) address insertions and deletions, use the **debug smf updates** command. To disable debugging output, use the **no** form of this command.

debug smf updates

no debug smf updates

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to debug SMF updates:

```
Switch# debug smf updates
Software MAC filter address insertions and deletions debugging is on
Switch#
```

Related Commands **undebug smf** (same as **no debug smf**)

debug spanning-tree

To debug spanning tree activities, use the **debug spanning-tree** command. To disable debugging output, use the **no** form of this command.

```
debug spanning-tree {all | bpdud | bpdud-opt | etherchannel | config | events | exceptions |
  general | mst | pvst+ | root | snmp}
```

```
no debug spanning-tree {all | bpdud | bpdud-opt | etherchannel | config | events | exceptions |
  general | mst | pvst+ | root | snmp}
```

Syntax Description

all	Displays all spanning tree debugging messages.
bpdud	Debugs spanning tree BPDU.
bpdud-opt	Debugs optimized BPDU handling.
etherchannel	Debugs spanning tree EtherChannel support.
config	Debugs spanning tree configuration changes.
events	Debugs TCAM events.
exceptions	Debugs spanning tree exceptions.
general	Debugs general spanning tree activity.
mst	Debugs multiple spanning tree events.
pvst+	Debugs PVST+ events.
root	Debugs spanning tree root events.
snmp	Debugs spanning tree SNMP events.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

This example shows how to debug spanning tree PVST+:

```
Switch# debug spanning-tree pvst+
Spanning Tree PVST+ debugging is on
Switch#
```

Related Commands

undebud spanning-tree (same as **no debug spanning-tree**)

debug spanning-tree backbonefast

To enable debugging of spanning tree BackboneFast events, use the **debug spanning-tree backbonefast** command. To disable debugging output, use the **no** form of this command.

debug spanning-tree backbonefast [detail | exceptions]

no debug spanning-tree backbonefast

Syntax Description	detail	(Optional) Displays detailed BackboneFast debugging messages.
	exceptions	(Optional) Enables debugging of spanning tree BackboneFast exceptions.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines This command is supported by the supervisor engine only and can be entered only from the switch console.

Examples This example shows how to enable debugging and to display detailed spanning tree BackboneFast debugging information:

```
Switch# debug spanning-tree backbonefast detail
Spanning Tree backbonefast detail debugging is on
Switch#
```

Related Commands **undebg spanning-tree backbonefast** (same as **no debug spanning-tree backbonefast**)

debug spanning-tree switch

To enable switch shim debugging, use the **debug spanning-tree switch** command. To disable debugging output, use the **no** form of this command.

```
debug spanning-tree switch {all | errors | general | pm | rx {decode | errors | interrupt | process } | state | tx [decode]}
```

```
no debug spanning-tree switch {all | errors | general | pm | rx {decode | errors | interrupt | process } | state | tx [decode]}
```

Syntax Description

all	Displays all spanning tree switch shim debugging messages.
errors	Enables debugging of switch shim errors or exceptions.
general	Enables debugging of general events.
pm	Enables debugging of port manager events.
rx	Displays received BPDU-handling debugging messages.
decode	Enables debugging of the decode received packets of the spanning tree switch shim.
errors	Enables debugging of the receive errors of the spanning tree switch shim.
interrupt	Enables shim ISR receive BPDU debugging on the spanning tree switch.
process	Enables process receive BPDU debugging on the spanning tree switch.
state	Enables debugging of the state changes on the spanning tree port.
tx	Enables transmit BPDU debugging on the spanning tree switch shim.
decode	(Optional) Enables decode transmitted packets debugging on the spanning tree switch shim.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

This command is supported only by the supervisor engine and can be entered only from the switch console.

Examples

This example shows how to enable transmit BPDU debugging on the spanning tree switch shim:

```
Switch# debug spanning-tree switch tx
Spanning Tree Switch Shim transmit bpdu debugging is on
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 303
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 304
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 305
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 349
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 350
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 351
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 801
<... output truncated...>
Switch#
```

Related Commands

undebug spanning-tree switch (same as **no debug spanning-tree switch**)

debug spanning-tree uplinkfast

To enable debugging of spanning tree UplinkFast events, use the **debug spanning-tree uplinkfast** command. To disable debugging output, use the **no** form of this command.

debug spanning-tree uplinkfast [exceptions]

no debug spanning-tree uplinkfast

Syntax Description	exceptions (Optional) Enables debugging of spanning tree UplinkFast exceptions.				
Defaults	This command has no default settings.				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(8a)EW</td> <td>Support for this command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Release	Modification				
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.				
Usage Guidelines	This command is supported only by the supervisor engine and can be entered only from the switch console.				
Examples	<p>This example shows how to debug spanning tree UplinkFast exceptions:</p> <pre>Switch# debug spanning-tree uplinkfast exceptions Spanning Tree uplinkfast exceptions debugging is on Switch#</pre>				
Related Commands	undebug spanning-tree uplinkfast (same as no debug spanning-tree uplinkfast)				

debug sw-vlan

To debug VLAN manager activities, use the **debug sw-vlan** command. To disable debugging output, use the **no** form of this command.

debug sw-vlan { **badpmcookies** | **events** | **management** | **packets** | **registries** }

no debug sw-vlan { **badpmcookies** | **events** | **management** | **packets** | **registries** }

Syntax Description	badpmcookies	Displays VLAN manager incidents of bad port-manager cookies.
	events	Debugs VLAN manager events.
	management	Debugs VLAN manager management of internal VLANs.
	packets	Debugs packet handling and encapsulation processes.
	registries	Debugs VLAN manager registries.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to debug software VLAN events:

```
Switch# debug sw-vlan events
vlan manager events debugging is on
Switch#
```

Related Commands **undebug sw-vlan** (same as **no debug sw-vlan**)

debug sw-vlan ifs

To enable VLAN manager IOS file system (IFS) error tests, use the **debug sw-vlan ifs** command. To disable debugging output, use the **no** form of this command.

```
debug sw-vlan ifs {open {read | write} | read {1 | 2 | 3 | 4} | write }
```

```
no debug sw-vlan ifs {open {read | write} | read {1 | 2 | 3 | 4} | write }
```

Syntax Description	Parameter	Description
	open	Enables VLAN manager IFS debugging of errors in an IFS file-open operation.
	read	Debugs errors that occurred when the IFS VLAN configuration file was open for reading.
	write	Debugs errors that occurred when the IFS VLAN configuration file was open for writing.
	{1 2 3 4}	Determines the file-read operation. See “Usage Guidelines” for information about operation levels.
	write	Debugs errors that occurred during an IFS file-write operation.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines The following are four types of file read operations:

- 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 TLV descriptor structures.
- Operation **4**—Reads TLV data.

Examples This example shows how to debug of TLV data errors during a file-read operation:

```
Switch# debug sw-vlan ifs read 4
vlan manager ifs read # 4 errors debugging is on
Switch#
```

Related Commands **undebg sw-vlan ifs** (same as **no debug sw-vlan ifs**)

debug sw-vlan notification

To enable debugging messages that trace the activation and deactivation of ISL VLAN IDs, use the **debug sw-vlan notification** command. To disable debugging output, use the **no** form of this command.

```
debug sw-vlan notification { accfwdchange | allowedvlanfgchange | fwdchange | linkchange | modechange | pruningfgchange | statechange }
```

```
no debug sw-vlan notification { accfwdchange | allowedvlanfgchange | fwdchange | linkchange | modechange | pruningfgchange | statechange }
```

Syntax Description		
	accfwdchange	Enables VLAN manager notification of aggregated access interface STP forward changes.
	allowedvlanfgchange	Enables VLAN manager notification of changes to allowed VLAN configuration.
	fwdchange	Enables VLAN manager notification of STP forwarding changes.
	linkchange	Enables VLAN manager notification of interface link state changes.
	modechange	Enables VLAN manager notification of interface mode changes.
	pruningfgchange	Enables VLAN manager notification of changes to pruning configuration.
	statechange	Enables VLAN manager notification of interface state changes.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to debug the software VLAN interface mode change notifications:

```
Switch# debug sw-vlan notification modechange
vlan manager port mode change notification debugging is on
Switch#
```

Related Commands **undebug sw-vlan notification** (same as **no debug sw-vlan notification**)

debug sw-vlan vtp

To enable debugging messages to be generated by the VTP protocol code, use the **debug sw-vlan vtp** command. To disable debugging output, use the **no** form of this command.

debug sw-vlan vtp {events | packets | pruning [packets | xmit] | xmit }

no debug sw-vlan vtp {events | packets | pruning [packets | xmit] | xmit }

Syntax Description	events	Displays general-purpose logic flow and detailed VTP debugging messages generated by the VTP_LOG_RUNTIME macro in the VTP code.
	packets	Displays the contents of all incoming VTP packets that have been passed into the VTP code from the IOS VTP platform-dependent layer, except for pruning packets.
	pruning	Enables debugging message to be generated by the pruning segment of the VTP protocol code.
	packets	(Optional) Displays the contents of all incoming VTP pruning packets that have been passed into the VTP code from the IOS VTP platform-dependent layer.
	xmit	(Optional) Displays the contents of all outgoing VTP packets that the VTP code will request the IOS VTP platform-dependent layer to send.
	xmit	Displays the contents of all outgoing VTP packets that the VTP code will request the IOS VTP platform-dependent layer to send; does not include pruning packets.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines If you do not enter any more parameters after entering **pruning**, the VTP pruning debugging messages are displayed.

Examples This example shows how to debug software VLAN outgoing VTP packets:

```
Switch# debug sw-vlan vtp xmit
vtp xmit debugging is on
Switch#
```

Related Commands **undebug sw-vlan vtp** (same as **no debug sw-vlan vtp**)

debug uddl

To enable debugging of UDLD activity, use the **debug uddl** command. To disable debugging output, use the **no** form of this command.

debug uddl {events | packets | registries}

no debug uddl {events | packets | registries}

Syntax Description	events	Enables debugging of UDLD process events as they occur.
	packets	Enables debugging of the UDLD process as it receives packets from the packet queue and attempts to transmit packets at the request of the UDLD protocol code.
	registries	Enables debugging of the UDLD process as it processes registry upcalls from the UDLD process-dependent module and other feature modules.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines This command is supported by the supervisor engine only and can be entered only from the Catalyst4500 series switch console.

Examples This example shows how to enable debugging of UDLD events:

```
Switch# debug uddl events
UDLD events debugging is on
Switch#
```

This example shows how to enable debugging of UDLD packets:

```
Switch# debug uddl packets
UDLD packets debugging is on
Switch#
```

This example shows how to enable debugging of UDLD registry events:

```
Switch# debug uddl registries
UDLD registries debugging is on
Switch#
```

Related Commands **undebug uddl** (same as **no debug uddl**)

debug vqpc

To debug VLAN Query Protocol (VQP), use the **debug vqpc** command. To disable debugging output, use the **no** form of this command.

debug vqpc [**all** | **cli** | **events** | **learn** | **packet**]

no debug vqpc [**all** | **cli** | **events** | **learn** | **packet**]

Syntax Description		
	all	(Optional) Debugs all VQP events.
	cli	(Optional) Debugs VQP command line interface.
	events	(Optional) Debugs VQP events.
	learn	(Optional) Debugs VQP address learning.
	packet	(Optional) Debugs VQP packets.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to enable all PM debugging:

```
Switch# debug vqpc all
Switch#
```

Related Commands [vmps reconfirm \(privileged EXEC\)](#)

define interface-range

To create a macro of interfaces, use the **define interface-range** command.

```
define interface-range macro-name interface-range
```

Syntax Description	
<i>macro-name</i>	Name of the interface range macro; up to 32 characters.
<i>interface-range</i>	List of valid ranges when specifying interfaces; see “Usage Guidelines.”

Defaults This command has no default settings.

Command Modes Global configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines The macro name is a character string of up to 32 characters.
A macro can contain up to five ranges. An interface range cannot span modules.

When entering the *interface-range*, use these formats:

- *interface-type* {*mod*}/{*first-interface*} - {*last-interface*}
- *interface-type* {*mod*}/{*first-interface*} - {*last-interface*}

Valid values for *interface-type* are as follows:

- **FastEthernet**
- **GigabitEthernet**
- **Vlan** *vlan_id*

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

```
Switch(config)# define interface-range macro1 gigabitethernet 4/1-6, fastethernet 2/1-5
Switch(config)#
```

Related Commands [interface range](#)

deny

To deny an ARP packet based on matches against the DHCP bindings, use the **deny** command. Use the **no** form of the command to remove specified ACEs from the access list.

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

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

Syntax Description

request	(Optional) Requests a match for the ARP request. When request is not specified, matching is performed against all ARP packets.
ip	Specifies the sender IP address.
any	Specifies that any IP or MAC address will be accepted.
host <i>sender-ip</i>	Specifies that only a specific sender IP address will be accepted.
<i>sender-ip sender-ip-mask</i>	Specifies that a specific range of sender IP addresses will be accepted.
mac	Specifies the sender MAC address.
host <i>sender-mac</i>	Specifies that only a specific sender MAC address will be accepted.
<i>sender-mac sender-mac-mask</i>	Specifies that a specific range of sender MAC addresses will be accepted.
response	Specifies a match for the ARP responses.
ip	Specifies the IP address values for the ARP responses.
host <i>target-ip</i>	(Optional) Specifies that only a specific target IP address will be accepted.
<i>target-ip target-ip-mask</i>	(Optional) Specifies that a specific range of target IP addresses will be accepted.
mac	Specifies the MAC address values for the ARP responses.
host <i>target-mac</i>	(Optional) Specifies that only a specific target MAC address will be accepted.
<i>target-mac target-mac-mask</i>	(Optional) Specifies that a specific range of target MAC addresses will be accepted.
log	(Optional) Logs a packet when it matches the access control entry (ACE).

Defaults

At the end of the ARP access list, there is an implicit **deny ip any mac any** command.

Command Modes

arp-nacl configuration

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Deny clauses can be added to forward or drop ARP packets based on some matching criteria.

Examples A host with a MAC address of 0000.0000.abcd has an IP address of 1.1.1.1. To deny both requests and responses from this host, define an access list as follows:

```
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
Switch# show arp access-list

ARP access list static-hosts
    deny ip host 1.1.1.1 mac host 0000.0000.abcd
Switch#
```

Related Commands [arp access-list](#)
[ip arp inspection filter vlan](#)
[permit](#)

diagnostic monitor action

To direct the action of the switch when it detects a packet memory failure, use the **diagnostic monitor action** command.

diagnostic monitor action [**conservative** | **normal** | **aggressive**]

Syntax Description	conservative	(Optional) The bootup SRAM diagnostics log all failures and remove all affected buffers from the hardware operation. The ongoing SRAM diagnostics will log events, but will take no other action.
	normal	(Optional) The SRAM diagnostics operate as in conservative mode, except that an ongoing failure resets the supervisor engine. This action allows for the bootup tests to map out the affected memory.
	aggressive	(Optional) The SRAM diagnostics operate as in normal mode, except that a bootup failure only logs failures and does not allow the supervisor engine to come online. This action allows for either a redundant supervisor engine or network-level redundancy to take over.

Defaults normal mode

Command Modes Global configuration mode

Command History	Release	Modification
	12.2(18)EW	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Use the **conservative** keyword when you do not want the switch to reboot so that the problem can be fixed.

Use the **aggressive** keyword when you have redundant supervisor engines, or when network-level redundancy has been provided.

Examples This example shows how to configure the switch to initiate an RPR switchover when an ongoing failure occurs:

```
Switch# configure terminal
Switch (config)# diagnostic monitor action normal
```

Related Commands [show diagnostic result module test 2](#)
[show diagnostic result module test 3](#)

dot1x guest-vlan

To enable guest VLAN on a per-port basis use the **dot1x guest-vlan** command. To return to the default setting, use the **no** form of this command.

```
dot1x guest-vlan vlan-id
```

```
no dot1x guest-vlan vlan-id
```

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

Defaults	The default value for the guest VLAN is 0.
-----------------	--

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	Guest VLAN can be configured only on switch ports that are statically configured as an access port. Guest VLAN has the same restrictions as a dot1x port that has no trunk port, dynamic port, EtherChannel port, or SPAN destination port.
-------------------------	---

Examples	This example shows how to enable guest VLAN on Fast Ethernet interface 4/3:
-----------------	---

```
Switch# config terminal
Switch(config)# interface fastethernet4/3
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x guest-vlan 26
Switch(config-if)# end
Switch(config)# end
Switch#
```

Related Commands	dot1x max-reauth-req show dot1x
-------------------------	--

dot1x initialize

To unauthorize an interface before reinitializing 802.1x, use the **dot1x initialize** command.

dot1x initialize *interface*

Syntax Description	<i>interface</i>	The number of the interface.
---------------------------	------------------	------------------------------

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	Use this command to initialize state machines and to set up the environment for fresh authentication.
-------------------------	---

Examples	This example shows how to initialize the 802.1x state machines on an interface:
-----------------	---

```
Switch# dot1x initialize
Switch#
```

Related Commands	dot1x initialize show dot1x
-------------------------	--

dot1x max-reauth-req

To set the maximum number of times the switch will retransmit an EAP-Request/Identity frame to the client before restarting the authentication process, use the **dot1x max-reauth-req** command. To return to the default setting, use the **no** form of this command.

dot1x max-reauth-req *count*

no dot1x max-reauth-req

Syntax Description

count Number of times that the switch retransmits EAP-Request/Identity frames before restarting the authentication process; valid values are from 1 to 10.

Defaults

The switch sends a maximum of two retransmissions.

Command Modes

Interface configuration.

Command History

Release	Modification
12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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. This setting impacts the wait before a non-dot1x-capable client is admitted to the guest VLAN, if one is configured.

You can verify your settings by entering the **show dot1x** privileged EXEC command.

Examples

This example shows how to set 5 as the number of times that the switch retransmits an EAP-Request/Identity frame before restarting the authentication process:

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

Related Commands

[show dot1x](#)

dot1x max-req

To set the maximum number of times the switch retransmits an Extensible Authentication Protocol (EAP)-Request frame of types other than EAP-Request/Identity to the client before restarting the authentication process, use the **dot1x max-req** command. To return to the default setting, use the **no** form of this command.

dot1x max-req *count*

no dot1x max-req

Syntax Description	<i>count</i> Number of times that the switch retransmits EAP-Request frames of types other than EAP-Request/Identity before restarting the authentication process; valid values are from 1 to 10.
---------------------------	---

Defaults	The switch sends a maximum of two retransmissions.
-----------------	--

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(19)EW	This command was modified to control on EAP-Request/Identity retransmission limits.

Usage Guidelines	<p>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.</p> <p>You can verify your settings by entering the show dot1x privileged EXEC command.</p>
-------------------------	--

Examples	<p>This example shows how to set 5 as the number of times that the switch retransmits an EAP-Request frame before restarting the authentication process:</p>
-----------------	--

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

Related Commands	<p>dot1x initialize</p> <p>dot1x max-reauth-req</p> <p>show dot1x</p>
-------------------------	---

dot1x multiple-hosts

To allow multiple hosts (clients) on an 802.1x-authorized port that has the **dot1x port-control** interface configuration command set to **auto**, use the **dot1x multiple-hosts** command. To return to the default setting, use the **no** form of this command.

dot1x multiple-hosts

no dot1x multiple-hosts

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines This command enables you to attach multiple clients to a single 802.1x-enabled port. In this 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.

Examples This example shows how to enable 802.1x on Gigabit Ethernet 1/1 and to allow multiple hosts:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x multiple-hosts
```

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

Related Commands [show dot1x](#)

dot1x port-control

To enable manual control of the authorization state on a port, use the **dot1x port-control** command. To return to the default setting, use the **no** form of this command.

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

no dot1x port-control { **auto** | **force-authorized** | **force-unauthorized** }

Syntax Description

auto	Enables 802.1x authentication on the interface and causes 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	Disables 802.1x authentication on the interface and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1x-based authentication of the client.
force-unauthorized	Denies all access through the specified interface 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 interface.

Defaults

The port 802.1x authorization is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The 802.1x protocol is supported on both Layer 2 static-access ports and Layer 3-routed ports.

You can use the **auto** keyword only if the port is not configured as one of these:

- Trunk port—If you try to enable 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.
- 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, the port mode 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 an inactive port of an EtherChannel, the port does not join the EtherChannel.

- Switch Port Analyzer (SPAN) destination port—You can enable 802.1x on a port that is a SPAN destination port; however, 802.1x is disabled until the port is removed as a SPAN destination. You can enable 802.1x on a SPAN source port.

To globally disable 802.1x on the switch, you must disable it on each port. There is no global configuration command for this task.

Examples

This example shows how to enable 802.1x on Gigabit Ethernet 1/1:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# dot1x port-control auto
Switch#
```

You can verify your settings by using **show dot1x all** or **show dot1x interface int** to show the port-control status. An enabled status indicates that the port-control value is set either to **auto** or to **force-unauthorized**.

Related Commands

[show dot1x](#)

dot1x re-authenticate

To manually initiate a reauthentication of all 802.1x-enabled ports or the specified 802.1x-enabled port, use the **dot1x re-authenticate** command.

dot1x re-authenticate [**interface** *interface-id*]

Syntax Description	interface <i>interface-id</i> (Optional) Slot and port number of the interface.
---------------------------	--

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	You can use this command to reauthenticate a client without waiting for the configured number of seconds between reauthentication attempts (re-authperiod) and automatic reauthentication.
-------------------------	--

Examples	This example shows how to manually reauthenticate the device connected to Gigabit Ethernet interface 1/1:
-----------------	---

```
Switch# dot1x re-authenticate interface gigabitethernet1/1
Starting reauthentication on gigabitethernet1/1
Switch#
```


dot1x re-authentication

To enable periodic reauthentication of the client, use the **dot1x re-authentication** command. To return to the default setting, use the **no** form of this command.

dot1x re-authentication

no dot1x re-authentication

Syntax Description This command has no arguments or keywords.

Defaults The periodic reauthentication is disabled.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines You configure the amount of time between periodic reauthentication attempts by using the **dot1x timeout re-authperiod** global configuration command.

Examples This example shows how to disable periodic reauthentication of the client:

```
Switch(config-if)# no dot1x re-authentication
Switch(config-if)#
```

This example shows how to enable periodic reauthentication and set the number of seconds between reauthentication attempts to 4000 seconds:

```
Switch(config-if)# dot1x re-authentication
Switch(config-if)# dot1x timeout re-authperiod 4000
Switch#
```

You can verify your settings by entering the **show dot1x** privileged EXEC command.

Related Commands [dot1x timeout](#)
[show dot1x](#)

dot1x system-auth-control

To enable 802.1x authentication on the switch, use the **dot1x system-auth-control** command. To disable 802.1x authentication on the system, use the **no** form of this command.

dot1x system-auth-control

no dot1x system-auth-control

Syntax Description This command has no arguments or keywords.

Defaults The 802.1x authentication is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines You must enable **dot1x system-auth-control** if you want to use 802.1x access controls on any port on the switch. You can then use the **dot1x port-control auto** command on each specific port on which you want 802.1x access controls to be used.

Examples This example shows how to enable 802.1x authentication:

```
Switch(config)# dot1x system-auth-control
Switch(config)#
```

Related Commands [dot1x initialize](#)
[show dot1x](#)

dot1x timeout

To set the reauthentication timer, use the **dot1x timeout** command. To return to the default setting, use the **no** form of this command.

```
dot1x timeout { reauth-period seconds | quiet-period seconds | tx-period seconds |
supp-timeout seconds | server-timeout seconds }
```

```
no dot1x timeout { reauth-period | quiet-period | tx-period | supp-timeout | server-timeout }
```

Syntax Description

reauth-period <i>seconds</i>	Number of seconds between reauthentication attempts; valid values are from 1 to 65535. See “Usage Guidelines” for more information.
quiet-period <i>seconds</i>	Number of seconds the switch remains in the quiet state following a failed authentication exchange with the client; valid values are from 0 to 65535 seconds.
tx-period <i>seconds</i>	Number of seconds the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request; valid values are from 15 to 65535 seconds.
supp-timeout <i>seconds</i>	Number of seconds the switch waits for the retransmission of EAP-Request packets; valid values are from 30 to 65535 seconds.
server-timeout <i>seconds</i>	Number of seconds the switch waits for the retransmission of packets by the backend authenticator to the authentication server; valid values are from 30 to 65535 seconds.

Defaults

The default settings are as follows:

- Reauthentication period is 3600 seconds.
- Quiet period is 60 seconds.
- Transmission period is 30 seconds.
- Supplicant timeout is 30 seconds.
- Server timeout is 30 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(12)EW	Support for this command was introduced on the Catalyst4500 series switches.

Usage Guidelines

Periodic reauthentication must be enabled before entering the **dot1x timeout re-authperiod** command. Enter the **dot1x re-authentication** command to enable periodic reauthentication.

This example shows how to set 60 as the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request:

```
Switch(config-if)# dot1x timeout tx-period 60  
Switch(config-if)#
```

You can verify your settings by entering the **show dot1x** privileged EXEC command.

Related Commands

[dot1x initialize](#)
[show dot1x](#)

duplex

To configure the duplex operation on an interface, use the **duplex** command. To return to the default setting, use the **no** form of this command.

duplex {auto | full | half}

no duplex

Syntax Description

auto	Specifies autonegotiation operation.
full	Specifies full-duplex operation.
half	Specifies half-duplex operation.

Defaults

Half-duplex operation

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

[Table2-2](#) lists the supported command options by interface.

Table2-2 Supported duplex Command Options

Interface Type	Supported Syntax	Default Setting	Guidelines
10/100-Mbps module	duplex [half full]	half	If the speed is set to auto , you will not be able to set the duplex mode. If the speed is set to 10 or 100 , and you do not configure the duplex setting, the duplex mode is set to half duplex.
100-Mbps fiber modules	duplex [half full]	half	
Gigabit Ethernet Interface	Not supported.	Not supported.	Gigabit Ethernet interfaces are set to full duplex.
10/100/1000	duplex [half full]		If the speed is set to auto or 1000 , you will not be able to set duplex . If the speed is set to 10 or 100 , and you do not configure the duplex setting, the duplex mode is set to half duplex.

If the transmission speed on a 16-port RJ-45 Gigabit Ethernet port is set to **1000**, duplex mode is set to **full**. If the transmission speed is changed to **10** or **100**, the duplex mode stays at **full**. You must configure the correct duplex mode on the switch when the transmission speed changes to **10** or **100** from 1000 Mbps.

**Note**

Catalyst 4006 switches cannot automatically negotiate interface speed and duplex mode if either connecting interface is configured to a value other than **auto**.

**Caution**

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

Table2-3 describes the system performance for different combinations of the duplex and speed modes. The specified **duplex** command configured with the specified **speed** command produces the resulting action shown in the table.

Table2-3 Relationship Between duplex and speed Commands

duplex Command	speed Command	Resulting System Action
duplex half or duplex full	speed auto	Autonegotiates both speed and duplex modes
duplex half	speed 10	Forces 10 Mbps and half duplex
duplex full	speed 10	Forces 10 Mbps and full duplex
duplex half	speed 100	Forces 100 Mbps and half duplex
duplex full	speed 100	Forces 100 Mbps and full duplex
duplex full	speed 1000	Forces 1000 Mbps and full duplex

Examples

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

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

Related Commands

speed
interface (refer to Cisco IOS documentation)
show controllers (refer to Cisco IOS documentation)
show interfaces (refer to Cisco IOS documentation)

errdisable detect

To enable error disable detection, use the **errdisable detect** command. To disable the error disable detection feature, use the **no** form of this command.

```
errdisable detect cause { all | arp-inspection | dhcp-rate-limit | dtp-flap | gbic-invalid |
l2ptguard | link-flap | pagp-flap }
```

```
no errdisable detect cause { all | arp-inspection | dhcp-rate-limit | dtp-flap | gbic-invalid |
l2ptguard | link-flap | pagp-flap }
```

Syntax Description

cause	Specifies error disable detection to detect from a specific cause.
all	Specifies error disable detection for all error-disable causes.
arp-inspection	Specifies detection for the ARP inspection error-disable cause.
dhcp-rate-limit	Specifies detection for the DHCP rate limit error-disable cause.
dtp-flap	Specifies detection for the DTP flap error-disable cause.
gbic-invalid	Specifies detection for the GBIC invalid error-disable cause.
l2ptguard	Specifies detection for the Layer 2 protocol-tunnel error-disable cause.
link-flap	Specifies detection for the link flap error-disable cause.
pagp-flap	Specifies detection for the PAgP flap error-disable cause.

Defaults

All error disable causes are detected.

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

A cause (dtp-flap, link-flap, pagp-flap) is defined as the reason 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).

You must enter the **shutdown** command and then the **no shutdown** command to recover an interface manually from error disable.

Examples

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

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

To disable error disable detection for DAI, perform the following:

```
Switch(config)# no errdisable detect cause arp-inspection
Switch(config)# end
Switch# show errdisable detect
ErrDisable Reason      Detection status
-----
udld                    Enabled
bpduguard               Enabled
security-violatio      Enabled
channel-misconfig      Disabled
psecure-violation      Enabled
vmps                    Enabled
pagp-flap              Enabled
dtp-flap                Enabled
link-flap               Enabled
l2ptguard              Enabled
gbic-invalid            Enabled
dhcp-rate-limit        Enabled
unicast-flood           Enabled
storm-control           Enabled
ilpower                 Enabled
arp-inspection         Disabled
Switch#
```

Related Commands

[show errdisable detect](#)
[show interfaces status](#)

errdisable recovery

To configure the recovery mechanism variables, use the **errdisable recovery** command. To return to the default setting, use the **no** form of this command.

```
errdisable recovery [cause {all | arp-inspection | bpduguard | channel-misconfig |
dhcp-rate-limit | dtp-flap | gbic-invalid | l2ptguard | link-flap | pagp-flap |
psecure-violation | security-violation | storm-control | udld | unicastflood | vmps}
[arp-inspection] [interval {interval}]]
```

```
no errdisable recovery [cause {all | arp-inspection | bpduguard | channel-misconfig |
dhcp-rate-limit | dtp-flap | gbic-invalid | l2ptguard | link-flap | pagp-flap |
psecure-violation | security-violation | storm-control | udld | unicastflood | vmps}
[arp-inspection] [interval {interval}]]
```

Syntax Description

cause	(Optional) Enables error disable recovery to recover from a specific cause.
all	(Optional) Enables the recovery timers for all error disable causes.
arp-inspection	(Optional) Enables the recovery timer for the ARP inspection cause.
bpduguard	(Optional) Enables the recovery timer for the BPDU guard error-disable cause.
channel-misconfig	(Optional) Enables the recovery timer for the channel-misconfig error-disable cause.
dhcp-rate-limit	(Optional) Enables the recovery timer for the DHCP rate limit error-disable cause.
dtp-flap	(Optional) Enables the recovery timer for the DTP flap error-disable cause.
gbic-invalid	(Optional) Enables the recovery timer for the GBIC invalid error-disable cause.
l2ptguard	(Optional) Enables the recovery timer for the Layer 2 protocol-tunnel error-disable cause.
link-flap	(Optional) Enables the recovery timer for the link flap error-disable cause.
pagp-flap	(Optional) Enables the recovery timer for the PAgP flap error-disable cause.
psecure-violation	(Optional) Enables the recovery timer for the psecure violation error-disable cause.
security-violation	(Optional) Enables automatic recovery of ports disabled due to 802.1x security violations.
storm-control	(Optional) Enable timer to recover from storm-control error-disable state.
udld	(Optional) Enables the recovery timer for the UDLD error-disable cause.
unicastflood	(Optional) Enables the recovery timer for the Unicast flood error-disable cause.
vmps	(Optional) Enables the recovery timer for the VMPS error-disable cause.
arp-inspection	(Optional) Enables ARP inspection cause and recovery timeout.
interval <i>interval</i>	(Optional) Specifies the time to recover from specified error-disable cause; valid values are from 30 to 86400 seconds.

Defaults

Error disable recovery is disabled.
The recovery interval is set to 300 seconds.

Command Modes

Configuration

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(19)EW	Support for the storm-control feature.

Usage Guidelines

A cause (bpduguard, dtp-flap, link-flap, pagp-flap, udld) is defined as the reason 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 error-disable recovery for the cause, the interface stays in error-disabled state until a shutdown and no shutdown occurs. If you enable recovery for a cause, the interface is brought out of error-disabled state and allowed to retry operation again once all the causes have timed out.

You must enter the **shutdown** command and then the **no shutdown** command to recover an interface manually from error disable.

Examples

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

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

This example shows how to set the timer to 300 seconds:

```
Switch(config)# errdisable recovery interval 300
Switch(config)#
```

To enable errdisable recovery for arp-inspection, do the following:

```
Switch(config)# errdisable recovery cause arp-inspection
Switch(config)# end
Switch# show errdisable recovery
ErrDisable Reason      Timer Status
-----
udld                    Disabled
bpduguard               Disabled
security-violatio      Disabled
channel-misconfig      Disabled
vmps                    Disabled
pagp-flap               Disabled
dtp-flap                Disabled
link-flap               Disabled
l2ptguard               Disabled
psecure-violation      Disabled
gbic-invalid            Disabled
dhcp-rate-limit        Disabled
unicast-flood           Disabled
storm-control           Disabled
arp-inspection          Enabled
```

```
Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:

Switch#
```

Related Commands

[show errdisable recovery](#)
[show interfaces status](#)

flowcontrol

To configure a Gigabit Ethernet interface to send or receive pause frames, use the **flowcontrol** command. To disable the flow control setting, use the **no** form of this command.

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

no flowcontrol { **receive** | **send** } { **off** | **on** | **desired** }

Syntax Description

receive	Specifies that the interface processes pause frames.
send	Specifies that the interface sends pause frames.
off	Prevents a local port from receiving and processing pause frames from remote ports or from sending pause frames to remote ports.
on	Enables a local port to receive and process pause frames from remote ports or send pause frames to remote ports.
desired	Obtains predictable results whether a remote port is set to on, off, or desired.

Defaults

The default settings for Gigabit Ethernet interfaces are as follows:

- Sending pause frames is desired—Gigabit Ethernet interfaces.
- Receiving pause frames is off—Gigabit Ethernet interfaces.
- Sending pause frames is on—oversubscribed Gigabit Ethernet interfaces.
- Receiving pause frames is desired—oversubscribed Gigabit Ethernet interfaces

[Table2-4](#) shows the default settings for modules:

Table2-4 Default Module Settings

Module	Ports	Send
All modules except WS-X4418-GB, WS-X4412-2GB-TX, and WS-X4416-2GB-TX	All ports except for the oversubscribed ports (1–18)	No
WS-X4418-GB	Uplink ports (1–2)	No
WS-X4418-GB	Oversubscribed ports (3–18)	Yes
WS-X4412-2GB-TX	Uplink ports (13–14)	No
WS-X4412-2GB-TX	Oversubscribed ports (1–12)	Yes
WS-X4416-2GB-TX	Uplink ports (17–18)	No

Command Modes

Interface configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Pause frames are special packets that signal a source to stop sending frames for a specific period of time because the buffers are full.

[Table2-5](#) describes guidelines for using different configurations of the **send** and **receive** keywords with the **flowcontrol** command.

Table2-5 Keyword Configurations for send and receive

Configuration	Description
send on	Enables a local port to send pause frames to remote ports. To obtain predictable results, use send on only when remote ports are set to receive on or receive desired .
send off	Prevents a local port from sending pause frames to remote ports. To obtain predictable results, use send off only when remote ports are set to receive off or receive desired .
send desired	Obtains predictable results whether a remote port is set to receive on , receive off , or receive desired .
receive on	Enables a local port to process pause frames that a remote port sends. To obtain predictable results, use receive on only when remote ports are set to send on or send desired .
receive off	Prevents remote ports from sending pause frames to local port. To obtain predictable results, use send off only when remote ports are set to receive off or receive desired .
receive desired	Obtains predictable results whether a remote port is set to send on , send off , or send desired .

[Table2-6](#) identifies how flow control will be forced or negotiated on Gigabit Ethernet interfaces based on their speed settings.



Note Catalyst 4006 switches support flow control only on gigabit interfaces.

Table2-6 Send Capability by Switch Type, Module, and Port

Interface Type	Configured Speed	Advertised Flow Control
10/100/1000BASE-TX	Speed 1000	Configured flow control always
1000BASE-T	Negotiation always enabled	Configured flow control always negotiated
1000BASE-X	No speed nonegotiation	Configured flow control negotiated
1000BASE-X	Speed nonegotiation	Configured flow control forced

Examples

This example shows how to enable send flow control:

```
Switch(config-if)# flowcontrol receive on  
Switch(config-if)#
```

This example shows how to disable send flow control:

```
Switch(config-if)# flowcontrol send off  
Switch(config-if)#
```

This example shows how to set receive flow control to desired:

```
Switch(config-if)# flowcontrol receive desired  
Switch(config-if)#
```

Related Commands

interface port-channel

interface range

interface vlan

show flowcontrol

show running-config (refer to Cisco IOS Documentation)

speed

hw-module power

To turn the power off on a slot or line module, use the **no hw-module power** command. To turn the power back on, use the **hw-module power** command.

hw-module [**slot** | **module**] *number* **power**

no hw-module [**slot** | **module**] *number* **power**

Syntax Description	slot	(Optional) Specifies a slot on a chassis.
	module	(Optional) Specifies a line module.
	number	(Optional) Specifies the slot or module number.

Defaults After a boot up, the power is on.

Command Modes Global configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(18)EW	Add slot and module keywords.

Examples This example shows how to shut off power to a module in slot 5:

```
Switch# no hw-module slot 5 power
Switch#
```

Related Commands [clear hw-module slot password](#)

instance

To map a VLAN or a set of VLANs to an MST instance, use the **instance** command. To return the VLANs to the common instance default, use the **no** form of this command.

```
instance instance-id { vlan vlan-range }
```

```
no instance instance-id
```

Syntax Description		
	<i>instance-id</i>	MST instance to which the specified VLANs are mapped; valid values are from 0 to 15.
	vlan <i>vlan-range</i>	Specifies the number of the VLANs to be mapped to the specified instance. The number is entered as a single value or a range; valid values are from 1 to 4094.

Defaults Mapping is disabled.

Command Modes MST configuration

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines The mapping is incremental, not absolute. This means that when you enter a range of VLANs, this range is added or removed to the existing ones.

Any unmapped VLAN is mapped to the CIST instance.

Examples This example shows how to map a range of VLANs to instance 2:

```
Switch(config-mst)# instance 2 vlans 1-100
Switch(config-mst)#
```

This example shows how to map a VLAN to instance 5:

```
Switch(config-mst)# instance 5 vlans 1100
Switch(config-mst)#
```

This example shows how to move a range of VLANs from instance 2 to the CIST instance:

```
Switch(config-mst)# no instance 2 vlans 40-60
Switch(config-mst)#
```

This example shows how to move all the VLANs mapped to instance 2 back to the CIST instance:

```
Switch(config-mst)# no instance 2
Switch(config-mst)#
```

Related Commands

[name](#)
[revision](#)
[show spanning-tree mst](#)
[spanning-tree mst configuration](#)

■ instance

interface port-channel

To access or create a port channel interface, use the **interface port-channel** command.

interface port-channel *channel-group*

Syntax Description	<i>channel-group</i> Port channel group number; valid values are from 1 to 64.
---------------------------	--

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	You do not have to create a port channel interface before assigning a physical interface to a channel group. A port channel interface is created automatically when the channel group gets its first physical interface, if it is not already created.
-------------------------	--

You can also create port channels by entering the **interface port-channel** command. This will create a Layer 3 port channel. To change the Layer 3 port channel into a Layer 2 port channel, use the **switchport** command before you assign physical interfaces to the channel group. A port channel cannot be changed from Layer 3 to Layer 2 or vice versa when it contains member ports.

Only one port channel in a channel group is allowed.



Caution

The Layer 3 port channel interface is the routed interface. Do not enable Layer 3 addresses on the physical Fast Ethernet interfaces.

If you want to use CDP, you must configure it only on the physical Fast Ethernet interface and not on the port-channel interface.

Examples	This example creates a port channel interface with a channel group number of 64:
-----------------	--

```
Switch(config)# interface port-channel 64
Switch(config)#
```

Related Commands	channel-group show etherchannel
-------------------------	--

interface range

To run a command on multiple ports at the same time, use the **interface range** command.

```
interface range { vlan vlan_id - vlan_id } { port-range | macro name }
```

Syntax Description		
vlan <i>vlan_id - vlan_id</i>	Specifies a VLAN range; valid values are from 1 to 4094.	
<i>port-range</i>	Port range; for a list of valid values for <i>port-range</i> , see “Usage Guidelines.”	
macro <i>name</i>	Specifies the name of a macro.	

Defaults This command has no default settings.

Command Modes Global configuration
Interface configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended VLAN addresses added.

Usage Guidelines You can use the **interface range** command on existing VLAN SVIs only. To display VLAN SVIs, enter the **show running config** command. VLANs not displayed cannot be used in the **interface range** command.

The values entered with the **interface range** command are applied to all existing VLAN SVIs.

Before you can use a macro, you must define a range using the **define interface-range** command.

All configuration changes made to a port range are saved to NVRAM, but port ranges created with the **interface range** command do not get saved to NVRAM.

You can enter the port range in two ways:

- Specifying up to five port ranges
- Specifying a previously defined macro

You can either specify the ports or the name of a port-range macro. A port range must consist of the same port type, and the ports within a range cannot span modules.

You can define up to five port ranges on a single command; separate each range with a comma.

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

```
interface range gigabitethernet 5/1 -20, gigabitethernet4/5 -20.
```

Use these formats when entering the *port-range*:

- *interface-type* {*mod*}/{*first-port*} - {*last-port*}
- *interface-type* {*mod*}/{*first-port*} - {*last-port*}

Valid values for *interface-type* are as follows:

- **FastEthernet**
- **GigabitEthernet**
- **Vlan** *vlan_id*

You cannot specify both a macro and an interface range in the same command. After creating a macro, you can enter additional ranges. Likewise, if you have already entered an interface range, the CLI does not allow you to enter a macro.

You can specify a single interface in the *port-range* value. This makes the command similar to the **interface** *interface-number* command.

Examples

This example shows how to use the **interface range** command to interface to FE 5/18 - 20:

```
Switch(config)# interface range fastethernet 5/18 - 20
Switch(config-if)#
```

This command shows how to run a port-range macro:

```
Switch(config)# interface range macro macrol
Switch(config-if)#
```

Related Commands

[define interface-range](#)

show running config (refer to Cisco IOS documentation)

interface vlan

To create or access a Layer 3 switch virtual interface (SVI), use the **interface vlan** command. To delete an SVI, use the **no** form of this command.

interface vlan *vlan_id*

no interface vlan *vlan_id*

Syntax Description	<i>vlan_id</i> Number of the VLAN; valid values are from 1 to 4094.
---------------------------	---

Defaults	Fast EtherChannel is not specified.
-----------------	-------------------------------------

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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended addressing was added.

Usage Guidelines	<p>SVIs are created the first time you enter the interface vlan <i>vlan_id</i> command for a particular VLAN. The <i>vlan_id</i> value 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. A message is displayed whenever a VLAN interface is newly created, so you can check that you entered the correct VLAN number.</p>
-------------------------	---

If you delete an SVI by entering the **no interface vlan** *vlan_id* command, the associated interface is forced into an administrative down state and marked as deleted. The deleted interface will no longer be visible in a **show interface** 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.

Examples	This example shows the output when you enter the interface vlan <i>vlan_id</i> command for a new VLAN number:
-----------------	--

```
Switch(config)# interface vlan 23
% Creating new VLAN interface.
Switch(config)#
```

ip arp inspection filter vlan

To permit ARPs from hosts configured for static IP when DAI is enabled and to define an ARP access list and apply it to a VLAN, use the **ip arp inspection filter vlan** command. Use the **no** form of this command to disable this application.

ip arp inspection filter *arp-acl-name* **vlan** *vlan-range* [*static*]

no ip arp inspection filter *arp-acl-name* **vlan** *vlan-range* [*static*]

Syntax Description

<i>arp-acl-name</i>	Access control list name.
<i>vlan-range</i>	VLAN number or range; valid values are from 1 to 4094.
<i>static</i>	(Optional) Specifies that the access control list should be applied statically.

Defaults

No defined ARP ACLs are applied to any VLAN.

Command Modes

Configuration

Command History

Release	Modification
12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

When an ARP access control list is applied to a VLAN for dynamic ARP inspection, ARP packets containing only IP-to-Ethernet MAC bindings are compared against the ACLs. All other packet types are bridged in the incoming VLAN without validation.

This command specifies that incoming ARP packets are compared against the ARP access control list, and packets are permitted only if the access control list permits them.

If access control lists deny packets because of explicit denies, the packets are dropped. If packets are denied because of an implicit deny, they are then matched against the list of DHCP bindings if the ACL is not applied statically.

Examples

This example shows how to apply the ARP ACL “static-hosts” to VLAN 1 for DAI:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip arp inspection filter static-hosts vlan 1
Switch(config)# end
Switch#
Switch# show ip arp inspection vlan 1
Source Mac Validation      : Enabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
```

ip arp inspection filter vlan

```

Vlan      Configuration      Operation      ACL Match      Static ACL
-----      -
      1      Enabled      Active      static-hosts      No

Vlan      ACL Logging      DHCP Logging
-----      -
      1      Acl-Match      Deny

Switch#

```

Related Commands

[arp access-list](#)
[show ip arp inspection](#)

ip arp inspection limit (interface)

To limit the rate of incoming ARP requests and responses on an interface and prevent DAI from consuming all of the system's resources in event of a DOS attack, use the **ip arp inspection limit** command. Use the **no** form of this command to release the limit.

ip arp inspection limit {rate *pps* | none} [**burst interval** *seconds*]

no ip arp inspection limit

Syntax Description		
	rate <i>pps</i>	Specifies an upper limit on the number of incoming packets processed per second. The rate can range from 1 to 10000.
	none	Specifies no upper limit on the rate of incoming ARP packets that can be processed.
	burst interval <i>seconds</i>	(Optional) Specifies the consecutive interval in seconds, over which the interface is monitored for high rate of ARP packets. The interval is configurable from 1 to 15 seconds.

Defaults

The rate is set to 15 packets per second 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.

Burst interval is set to 1 second by default.

Command Modes

Interface

Command History

Release	Modification
12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(20)EW	Added support for interface monitoring.

Usage Guidelines

Trunk ports should be configured with higher rates to reflect their aggregation. When the rate of incoming packets exceeds the user-configured rate, the interface is placed into an error-disabled state. The error-disable timeout feature can be used to remove the port from the error-disabled state. The rate applies to both trusted and nontrusted interfaces. Configure appropriate rates on trunks to handle packets across multiple DAI-enabled VLANs or use the **none** keyword to make the rate unlimited.

The rate of incoming ARP packets on channel ports is equal to the sum of the incoming rate of packets from all the channel members. Configure the rate limit for channel ports only after examining the rate of incoming ARP packets on the channel members.

After a switch receives more than the configured rate of packets every second consecutively over a period of burst seconds, the interface is placed into an error-disabled state.

Examples

This example shows how to limit the rate of incoming ARP requests to 25 packets per second:

```
Switch# config terminal
Switch(config)# interface fa6/3
Switch(config-if)# ip arp inspection limit rate 25
Switch(config-if)# end
Switch# show ip arp inspection interfaces fastEthernet 6/3
Interface      Trust State      Rate (pps)
-----
Fa6/3          Trusted          25
Switch#
```

This example shows how to limit the rate of incoming ARP requests to 20 packets per second and to set the interface monitoring interval to 5 consecutive seconds:

```
Switch# config terminal
Switch(config)# interface fa6/1
Switch(config-if)# ip arp inspection limit rate 20 burst interval 5
Switch(config-if)# end
```

Related Commands

[show ip arp inspection](#)

ip arp inspection log-buffer

To configure parameters that are associated with the logging buffer, use the **ip arp inspection log-buffer** command. Use the **no** form of this command to disable the parameters.

ip arp inspection log-buffer { *entries number* | *logs number interval seconds* }

no ip arp inspection log-buffer { *entries* | *logs* }

Syntax Description	Parameter	Description
	entries number	The number of entries from the logging buffer. The range is 0 to 1024.
	logs number	The number of entries to be logged in an interval. The range is 0 to 1024. A 0 value indicates that entries should not be logged out of this buffer.
	interval seconds	The logging rate. The range is 0 to 86400 (1 day). A 0 value represents an immediate log.

Defaults

When dynamic ARP inspection is enabled, denied, or dropped, ARP packets are logged.

The number of entries is set to 32.

The number of logging entries is limited to 5 per second.

The interval is set to 1.

Command Modes

Configuration

Command History

Release	Modification
12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The first dropped packet of a given flow is logged immediately. Subsequent packets for the same flow are registered but not logged immediately. Registering these packets is done in a log buffer that is shared by all VLANs. Entries from this buffer are logged on a rate-controlled basis.

Examples

This example shows how to configure the logging buffer to hold up to 45 entries:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip arp inspection log-buffer entries 45
Switch(config)# end
Switch# show ip arp inspection log
Total Log Buffer Size : 45
Syslog rate : 5 entries per 1 seconds.
No entries in log buffer.
Switch#
```

This example shows how to configure the logging rate to 10 logs per 3 seconds:

```
Switch(config)# ip arp inspection log-buffer logs 10 interval 3
Switch(config)# end
Switch# show ip arp inspection log
Total Log Buffer Size : 45
Syslog rate : 10 entries per 3 seconds.
No entries in log buffer.
Switch#
```

Related Commands

[arp access-list](#)
[show ip arp inspection](#)

ip arp inspection trust

To set a per-port configurable trust state that determines the set of interfaces where incoming ARP packets are inspected, use the **ip arp inspection trust** command. Use the **no** form of this command to make interfaces untrusted.

ip arp inspection trust

no ip arp inspection trust

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Interface

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to configure an interface to be trusted:

```
Switch# config terminal
Switch(config)# interface fastEthernet 6/3
Switch(config-if)# ip arp inspection trust
Switch(config-if)# end
```

To verify the configuration, use the show form of the command:

```
Switch# show ip arp inspection interfaces fastEthernet 6/3

Interface          Trust State      Rate (pps)
-----
Fa6/3              Trusted          None
Switch#
```

Related Commands [show ip arp inspection](#)

ip arp inspection validate

To perform specific checks for ARP inspection, use the **ip arp inspection validate** command. Use the **no** form of this command to disable the checks.

ip arp inspection validate [src-mac] [dst-mac] [ip]

no ip arp inspection validate [src-mac] [dst-mac] [ip]

Syntax Description	
src-mac	(Optional) Checks the source MAC address in the Ethernet header against the sender's MAC address in the ARP body. This checking is done against both ARP requests and responses. Note When enabled, packets with different MAC addresses are classified as invalid and are dropped.
dst-mac	(Optional) Checks the destination MAC address in the Ethernet header against the target MAC address in ARP body. This checking is done for ARP responses. Note When enabled, packets with different MAC addresses are classified as invalid and are dropped.
ip	(Optional) Checks 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 checked in all ARP requests and responses and target IP addresses are checked only in ARP responses.

Defaults Checks are disabled.

Command Modes Configuration

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines When enabling the checks, specify at least one of the keywords (**src-mac**, **dst-mac**, and **ip**) on the command line. Each command overrides the configuration of the previous command; that is, if a command enables **src** and **dst mac** validations, and a second command enables IP validation only, the **src** and **dst mac** validations are disabled as a result of the second command.

The **no** form of the command disables only the specified checks. If none of the check 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
Switch(config)# end
Switch# show ip arp inspection vlan 1
Source Mac Validation      : Enabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
```

Vlan	Configuration	Operation	ACL Match	Static ACL
----	-----	-----	-----	-----
1	Enabled	Active		

Vlan	ACL Logging	DHCP Logging
----	-----	-----
1	Deny	Deny

```
Switch#
```

Related Commands

[arp access-list](#)
[show arp access-list](#)

ip arp inspection vlan

To enable dynamic ARP inspection (DAI) on a per-VLAN basis, use the **ip arp inspection vlan** command. Use the **no** form of this command to disable DAI.

ip arp inspection vlan *vlan-range*

no ip arp inspection vlan *vlan-range*

Syntax Description	<i>vlan-range</i> Specifies a VLAN number or range; valid values are from 1 to 4094.
---------------------------	--

Defaults	ARP inspection is disabled on all VLANs.
-----------------	--

Command Modes	Configuration
----------------------	---------------

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	You must specify on which VLANs to enable DAI. DAI may not function on the configured VLANs if they have not been created or if they are private.
-------------------------	---

Examples	This example shows how to enable DAI on VLAN 1:
-----------------	---

```
Switch(config)# ip arp inspection vlan 1
Switch(config)# end
Switch# show ip arp inspection vlan 1

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan      Configuration   Operation   ACL Match   Static ACL
----      -
      1      Enabled           Active
Vlan      ACL Logging      DHCP Logging
----      -
      1      Deny             Deny
Switch#
```

Related Commands	arp access-list show ip arp inspection
-------------------------	---

ip arp inspection vlan logging

To control the type of packets that are logged, use the **ip arp inspection vlan logging** command. 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
{ permit | all | none } }
```

```
no ip arp inspection vlan vlan-range logging { acl-match | dhcp-bindings }
```

Syntax Description

vlan-range	The number of the VLANs to be mapped to the specified instance. The number is entered as a single value or a range; valid values are from 1 to 4094.
acl-match	Specifies the logging criteria for packets that are dropped or permitted based on ACL matches.
matchlog	Specifies that logging of packets matched against ACLs is controlled by the matchlog keyword in the permit and deny access control entries of the ACL. Note By default, the matchlog keyword is not available on the ACEs. When the keyword is used, denied packets are not logged. Packets are logged only when they match against an ACE that has the matchlog keyword.
none	Specifies that ACL-matched packets are not logged.
dhcp-bindings	Specifies the logging criteria for packets dropped or permitted based on matches against the DHCP bindings.
permit	Specifies logging when permitted by DHCP bindings.
all	Specifies logging when permitted or denied by DHCP bindings.
none	Prevents all logging of packets permitted or denied by DHCP bindings.

Defaults

All denied or dropped packets are logged.

Command Modes

Configuration

Command History

Release	Modification
12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The **acl-match** and **dhcp-bindings** keywords merge with each other; that is, when you set an ACL match configuration, the DHCP bindings configuration is not disabled. The **no** form of the command can be used to reset some of the logging criteria to their defaults. If neither option is specified, all types of logging are reset to log on when ARP packets are denied. The two options available to you are:

- **acl-match**—Logging on ACL matches is reset to log on deny
- **dhcp-bindings**—Logging on DHCP binding compared is reset to log on deny

Examples

This example shows how to configure ARP inspection on VLAN 1 to log packets on matching against ACLs with the **logging** keyword:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip arp inspection vlan 1 logging acl-match matchlog
Switch(config)# end
Switch# show ip arp inspection vlan 1

Source Mac Validation      : Enabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

Vlan    Configuration      Operation  ACL Match      Static ACL
----    -
      1    Enabled          Active

Vlan    ACL Logging          DHCP Logging
----    -
      1    Acl-Match          Deny
Switch#
```

Related Commands

[arp access-list](#)
[show ip arp inspection](#)

ip cef load-sharing algorithm

To configure the load-sharing hash function so that the source TCP/UDP port, or the destination TCP/UDP port, or both can be included in the hash in addition to the source and destination IP addresses, use the **ip cef load-sharing algorithm** command. To revert back to the default, which does not include the ports, use the **no** form of this command.

```
ip cef load-sharing algorithm {include-ports {source source | destination dest} | original | tunnel | universal}
```

```
no ip cef load-sharing algorithm {include-ports {source source | destination dest} | original | tunnel | universal}
```

Syntax Description

include-ports	Specifies algorithm that includes Layer 4 ports.
source <i>source</i>	Specifies source port in the load-balancing hash functions.
destination <i>dest</i>	Specifies destination port in the load-balancing hash. Uses source and destination in hash functions.
original	Original algorithm; not recommended.
tunnel	Specifies algorithm for use in tunnel-only environments.
universal	Specifies the default IOS load-sharing algorithm.

Defaults

Default load-sharing algorithm is disabled.



Note

This option does not include the source or destination port in the load-balancing hash.

Command Modes

Global configuration

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The original algorithm, tunnel algorithm, and universal algorithm are routed through hardware. For software-routed packets, the algorithms are handled by the software. The **include-ports** option does not apply to software-switched traffic.

Examples

This example shows how to configure the IP CEF load-sharing algorithm that includes Layer 4 ports:

```
Switch(config)# ip cef load-sharing algorithm include-ports
Switch(config)#
```

Related Commands

[show ip cef vlan](#)

ip dhcp snooping

To enable DHCP snooping globally, use the **ip dhcp snooping** command. To disable DHCP snooping, use the **no** form of this command.

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
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines You must enable DHCP snooping globally before you can use DHCP snooping on a VLAN.

Examples This example shows how to enable DHCP snooping:

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

This example shows how to disable DHCP snooping:

```
Switch(config)# no ip dhcp snooping
Switch(config)#
```

Related Commands

- [ip dhcp snooping information option](#)
- [ip dhcp snooping limit rate](#)
- [ip dhcp snooping trust](#)
- [ip dhcp snooping vlan](#)
- [show ip dhcp snooping](#)
- [show ip dhcp snooping binding](#)

ip dhcp snooping binding

To set up and generate a DHCP binding configuration to restore bindings across reboots, use the **ip dhcp snooping binding** command. To disable the binding configuration, use the **no** form of this command.

ip dhcp snooping binding *mac-address* **vlan** *vlan-#* *ip-address* **interface** *interface* **expiry** *seconds*

no ip dhcp snooping binding *mac-address* **vlan** *vlan-#* *ip-address* **interface** *interface*

Syntax Description		
	<i>mac-address</i>	Specifies a MAC address.
	vlan <i>vlan-#</i>	Specifies a valid VLAN number.
	<i>ip-address</i>	Specifies an IP address.
	interface <i>interface</i>	Specifies an interface type and number.
	expiry <i>seconds</i>	Specifies the interval (in seconds) after which binding is no longer valid.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Whenever a binding is added or removed using this command, the binding database is marked as changed and a write is initiated.

Examples This example shows how to generate DHCP binding configuration on interface gi1/1 in VLAN 1 with an expiration time of 1000 seconds:

```
Switch# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface gi1/1 expiry 1000
```

Related Commands

- [ip dhcp snooping](#)
- [ip dhcp snooping information option](#)
- [ip dhcp snooping trust](#)
- [ip dhcp snooping vlan](#)
- [show ip dhcp snooping](#)
- [show ip dhcp snooping binding](#)

ip dhcp snooping database

To store the bindings generated by DHCP snooping, use the **ip dhcp snooping database** command. Use the **no** form of this command to either reset the timeout, reset the write-delay, or delete the agent specified by the URL.

ip dhcp snooping database {*url* | **timeout** *seconds* | **write-delay** *seconds*}

no ip dhcp snooping database {**timeout** | **write-delay** }

Syntax Description		
<i>url</i>	Specifies the URL in one of the following forms:	<ul style="list-style-type: none"> • tftp://<host>/<filename> • ftp://<user>:<password>@<host>/<filename> • rcp://<user>@<host>/<filename> • nvram:/<filename> • bootflash:/<filename>
timeout <i>seconds</i>	Specifies when to abort the database transfer process after a change to the binding database.	The minimum value of the delay is 15 seconds. 0 is defined as infinite duration.
write-delay <i>seconds</i>	Specifies the duration for which the transfer should be delayed after a change to the binding database.	

Defaults

The timeout value is set to 300 seconds (5 minutes).
The write-delay value is set to 300 seconds.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Because both NVRAM and bootflash have limited storage capacity, we recommend that you store a file on an TFTP server. When a file is stored in a remote location that is accessible through TFTP, an RPR redundant supervisor engine can take over the binding list when a switchover occurs.

You need to create an empty file at the configured URL on network-based URLs (such as TFTP and FTP) before the switch can write the set of bindings for the first time at the URL.

Examples

This example shows how to store a database file with the IP address 10.1.1.1 within a directory called directory. A file named file must be present on the TFTP server.

```
Switch# config terminal
Switch(config)# ip dhcp snooping database tftp://10.1.1.1/directory/file
Switch(config)# end
Switch# show ip dhcp snooping database
Agent URL : tftp://10.1.1.1/directory/file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : Yes
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts      :          1  Startup Failures :          0
Successful Transfers :          0  Failed Transfers :          0
Successful Reads    :          0  Failed Reads     :          0
Successful Writes   :          0  Failed Writes    :          0
Media Failures      :          0

Switch#
```

Related Commands

- [ip dhcp snooping](#)
- [ip dhcp snooping binding](#)
- [ip dhcp snooping information option](#)
- [ip dhcp snooping trust](#)
- [ip dhcp snooping vlan](#)
- [show ip dhcp snooping](#)
- [show ip dhcp snooping binding](#)

ip dhcp snooping information option

To enable DHCP option 82 data insertion, use the **ip dhcp snooping information option** command. To disable DHCP option 82 data insertion, use the **no** form of this command.

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
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to enable DHCP option 82 data insertion:

```
Switch(config)# ip dhcp snooping information option
Switch(config)#
```

This example shows how to disable DHCP option 82 data insertion:

```
Switch(config)# no ip dhcp snooping information option
Switch(config)#
```

Related Commands

- [ip dhcp snooping](#)
- [ip dhcp snooping limit rate](#)
- [ip dhcp snooping trust](#)
- [ip dhcp snooping vlan](#)
- [show ip dhcp snooping](#)
- [show ip dhcp snooping binding](#)

ip dhcp snooping limit rate

To configure the number of DHCP messages an interface can receive per second, use the **ip dhcp snooping limit rate** command. To disable DHCP snooping rate limiting, use the **no** form of this command.

ip dhcp snooping limit rate *rate*

no ip dhcp snooping limit rate

Syntax Description	<i>rate</i> Number of DHCP messages a switch can receive per second.
---------------------------	--

Defaults	DHCP snooping rate limiting is disabled.
-----------------	--

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	Normally, the rate limit applies to untrusted interfaces. If you want to set up rate limiting for trusted interfaces, keep in mind that trusted interfaces aggregate all DHCP traffic in the switch, and you will need to adjust the interfaces rate limit to a higher value.
-------------------------	---

Examples	This example shows how to enable DHCP message rate limiting:
-----------------	--

```
Switch(config-if)# ip dhcp snooping limit rate 150
Switch(config)#
```

This example shows how to disable DHCP message rate limiting:

```
Switch(config-if)# no ip dhcp snooping limit rate
Switch(config)#
```

Related Commands	ip dhcp snooping ip dhcp snooping information option ip dhcp snooping trust ip dhcp snooping vlan show ip dhcp snooping show ip dhcp snooping binding
-------------------------	--

ip dhcp snooping trust

To configure an interface as trusted for DHCP snooping purposes, use the **ip dhcp snooping trust** command. To configure an interface as untrusted, use the **no** form of this command.

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
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to enable DHCP snooping trust on an interface:

```
Switch(config-if)# ip dhcp snooping trust
Switch(config)#
```

This example shows how to disable DHCP snooping trust on an interface:

```
Switch(config-if)# no ip dhcp snooping trust
Switch(config)#
```

Related Commands

- [ip dhcp snooping](#)
- [ip dhcp snooping information option](#)
- [ip dhcp snooping limit rate](#)
- [ip dhcp snooping vlan](#)
- [show ip dhcp snooping](#)
- [show ip dhcp snooping binding](#)

ip dhcp snooping vlan

Use the **ip dhcp snooping vlan** command to enable DHCP snooping on a VLAN. To disable DHCP snooping on a VLAN, use the **no** form of this command.

ip dhcp snooping [*vlan number*]

no ip dhcp snooping [*vlan number*]

Syntax Description	vlan number (Optional) Single VLAN number or a range of VLANs; valid values are from 1 to 4094.
---------------------------	--

Defaults	DHCP snooping is disabled.
-----------------	----------------------------

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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	DHCP snooping is enabled on a VLAN only if both the global snooping and the VLAN snooping are enabled.
-------------------------	--

Examples This example shows how to enable DHCP snooping on a VLAN:

```
Switch(config)# ip dhcp snooping vlan 10
Switch(config)#
```

This example shows how to disable DHCP snooping on a VLAN:

```
Switch(config)# no ip dhcp snooping vlan 10
Switch(config)#
```

This example shows how to enable DHCP snooping on a group of VLANs:

```
Switch(config)# ip dhcp snooping vlan 10 55
Switch(config)#
```

This example shows how to disable DHCP snooping on a group of VLANs:

```
Switch(config)# no ip dhcp snooping vlan 10 55
Switch(config)#
```

■ ip dhcp snooping vlan

Related Commands

ip dhcp snooping
ip dhcp snooping information option
ip dhcp snooping limit rate
ip dhcp snooping trust
show ip dhcp snooping
show ip dhcp snooping binding

ip igmp filter

To control whether all hosts on a Layer2 interface can join one or more IP multicast groups by applying an IGMP profile to the interface, use the **ip igmp filter** command. To remove a profile from the interface, use the **no** form of this command

ip igmp filter *profile number*

no ip igmp filter

Syntax Description	<i>profile number</i> IGMP profile number to be applied; valid values are from 1 to 429496795.
---------------------------	--

Defaults	Profiles are not applied.
-----------------	---------------------------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	12.1(11b)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 an interface.
-----------------	--

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip igmp filter 22
Switch(config-if)#
```

Related Commands	ip igmp profile show ip igmp profile
-------------------------	---

ip igmp max-groups

To set the maximum number of IGMP groups that a Layer 2 interface can join, use the **ip igmp max-groups** command. To set the maximum back to the default, use the **no** form of this command.

ip igmp max-groups *number*

no ip igmp max-groups

Syntax Description	<i>number</i>	Maximum number of IGMP groups that an interface can join; valid values are from 0 to 4294967294.
---------------------------	---------------	--

Defaults	No maximum limit.
-----------------	-------------------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	12.1(11b)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	You can use ip igmp max-groups command only on Layer 2 physical interfaces; you cannot set IGMP maximum groups for routed ports, switch virtual interfaces (SVIs), or ports that belong to an EtherChannel group.
-------------------------	--

Examples	This example shows how to limit the number of IGMP groups that an interface can join to 25.
-----------------	---

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip igmp max-groups 25
Switch(config-if)
```

ip igmp profile

To create an IGMP profile, use the **ip igmp profile** command. To delete the IGMP profile, use the **no** form of this command.

ip igmp profile *profile number*

no ip igmp profile *profile number*

Syntax Description	<i>profile number</i> IGMP profile number being configured; valid values are from 1 to 4294967295.
---------------------------	--

Defaults	No profile created.
-----------------	---------------------

Command Modes	Global configuration IGMP profile configuration
----------------------	--

Command History	Release	Modification
	12.1(11b)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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

Related Commands	ip igmp filter show ip igmp profile
-------------------------	--

ip igmp query-interval

To configure the frequency that the switch sends IGMP host-query messages, use the **ip igmp query-interval** command. To return to the default frequency, use the **no** form of this command.

ip igmp query-interval *seconds*

no ip igmp query-interval

Syntax Description	<i>seconds</i> Frequency, in seconds, at which IGMP host query messages are transmitted; valid values depend on the IGMP snooping mode. See “Usage Guidelines” for more information.
---------------------------	--

Defaults	The query interval is set to 60 seconds.
-----------------	--

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	<p>If you use the default IGMP snooping configuration, the valid query interval values are from 1 to 65535 seconds. If you have changed the default configuration to support CGMP as the IGMP snooping learning method, the valid query interval values are from 1 to 300 seconds.</p>
-------------------------	--

The designated switch for a LAN is the only switch that sends IGMP host query messages. For IGMP version 1, the designated switch is elected according to the multicast routing protocol that runs on the LAN. For IGMP version 2, the designated querier is the lowest IP-addressed multicast switch on the subnet.

If no queries are heard for the timeout period (controlled by the **ip igmp query-timeout** command), the switch becomes the querier.



Note

Changing the timeout period may severely impact multicast forwarding.

Examples	This example shows how to change the frequency at which the designated switch sends IGMP host query messages:
-----------------	---

```
Switch(config-if)# ip igmp query-interval 120
Switch(config-if)#
```

Related Commands	<p>ip igmp query-timeout (refer to Cisco IOS documentation)</p> <p>ip pim query-interval (refer to Cisco IOS documentation)</p> <p>show ip igmp groups (refer to Cisco IOS documentation)</p>
-------------------------	--

ip igmp snooping

To enable IGMP snooping, use the **ip igmp snooping** command. To disable IGMP snooping, use the **no** form of this command.

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

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

Syntax Description		
tcn	(Optional)	Specifies topology change configurations.
flood	(Optional)	Specifies flooding the spanning tree table to the network when a topology change occurs.
query	(Optional)	Specifies the TCN query configurations.
count <i>count</i>	(Optional)	Specifies how often the spanning tree table is flooded; valid values are from 1 to 10.
solicit	(Optional)	Specifies an IGMP general query.

Defaults

IGMP snooping is enabled.

Command Modes

Global configuration

Interface configuration

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(11)EW	Support for flooding the spanning tree table was added.

Usage Guidelines

The **tcn flood** option applies only to Layer 2 switch ports and EtherChannels; it does not apply to routed ports, VLAN interfaces, or Layer 3 channels.

The **ip igmp snooping command** is disabled by default on multicast routers.



Note

You can use the **tcn flood** option in Interface configuration mode.

Examples

This example shows how to enable IGMP snooping:

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

This example shows how to disable IGMP snooping:

```
Switch(config)# no ip igmp snooping
Switch(config)#
```

This example shows how to enable flooding the spanning-tree table to the network after 9 topology changes have occurred:

```
Switch(config)# ip igmp snooping tcn flood query count 9
Switch(config)#
```

This example shows how to disable flooding the spanning-tree table to the network:

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

This example shows how to enable an IGMP general query:

```
Switch(config)# ip igmp snooping tcn query solicit
Switch(config)#
```

This example shows how to disable an IGMP general query:

```
Switch(config)# no ip igmp snooping tcn query solicit
Switch(config)#
```

Related Commands

[ip igmp snooping vlan immediate-leave](#)
[ip igmp snooping vlan mrouter](#)
[ip igmp snooping vlan static](#)

ip igmp snooping report-suppression

To enable report suppression, use the **ip igmp snooping report-suppression** command. To disable report suppression and forward reports to multicast devices, use the **no** form of this command.

ip igmp snooping report-suppression

no igmp snooping report-suppression

Syntax Description This command has no arguments or keywords.

Defaults IGMP snooping report-suppression is enabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines If the **ip igmp snooping report-suppression** command is disabled, all IGMP reports are forwarded to the multicast devices.

If the command is enabled, report suppression is done by IGMP snooping.

Examples This example shows how to enable report suppression:

```
Switch(config)# ip igmp snooping report-suppression
Switch(config)#
```

This example shows how to disable report suppression:

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

This example shows how to display the system status for report suppression:

```
Switch# show ip igmp snoop
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 is running in IGMP_ONLY mode on this Vlan
IGMP snooping report suppression is enabled on this Vlan
Switch#
```

■ ip igmp snooping report-suppression

Related Commands

ip igmp snooping vlan immediate-leave
ip igmp snooping vlan mrouter
ip igmp snooping vlan static

ip igmp snooping vlan

To enable IGMP snooping for a VLAN, use the **ip igmp snooping vlan** command. To disable IGMP snooping, use the **no** form of this command.

ip igmp snooping vlan *vlan-id*

no ip igmp snooping vlan *vlan-id*

Syntax Description	<i>vlan-id</i> Number of the VLAN; valid values are from 1 to 1001 and from 1006 to 4094.
---------------------------	---

Defaults	IGMP snooping is disabled.
-----------------	----------------------------

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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended addressing was added.

Usage Guidelines	Before you can enable IGMP snooping on the Catalyst 4006 switches, you must configure the VLAN interface for multicast routing.
-------------------------	---

This command is entered in VLAN interface configuration mode only.

The **ip igmp snooping vlan** command is disabled by default on multicast routers.

Examples	This example shows how to enable IGMP snooping on a VLAN:
-----------------	---

```
Switch(config)# ip igmp snooping vlan 200
Switch(config)#
```

This example shows how to disable IGMP snooping on a VLAN:

```
Switch(config)# no ip igmp snooping vlan 200
Switch(config)#
```

Related Commands	<p>ip igmp snooping vlan immediate-leave</p> <p>ip igmp snooping vlan mrouter</p> <p>ip igmp snooping vlan static</p>
-------------------------	---

ip igmp snooping vlan explicit-tracking

To enable per-VLAN explicit host tracking, use the **ip igmp snooping vlan explicit-tracking** command. To disable explicit host tracking, use the **no** form of this command.

ip igmp snooping vlan *vlan-id* explicit-tracking

no ip igmp snooping vlan *vlan-id* explicit-tracking

Syntax Description	<i>vlan_id</i> (Optional) Specifies a VLAN; valid values are from 1 to 1001 and from 1006 to 4094.
---------------------------	--

Defaults	Explicit host tracking is enabled.
-----------------	------------------------------------

Command Modes	Configuration
----------------------	---------------

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to disable IGMP explicit host tracking on interface VLAN 200 and how to verify the configuration:

```
Switch(config)# no ip igmp snooping vlan 200 explicit-tracking
Switch(config)# end
Switch# show ip igmp snooping vlan 200 | include explicit tracking
Global IGMP Snooping configuration:
-----
IGMP snooping           : Enabled
IGMPv3 snooping         : Enabled
Report suppression      : Enabled
TCN solicit query       : Disabled
TCN flood query count   : 2

Vlan 2:
-----
IGMP snooping           : Enabled
IGMPv2 immediate leave  : Disabled
Explicit host tracking    : Disabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode : IGMP_ONLY
Explicit host tracking    : Disabled
Switch#
```

Related Commands	clear ip igmp snooping statistics vlan (refer to Cisco IOS documentation) show ip igmp snooping membership show ip igmp snooping statistics vlan (refer to Cisco IOS documentation)
-------------------------	--

ip igmp snooping vlan immediate-leave

To enable IGMP immediate-leave processing, use the **ip igmp snooping vlan immediate-leave** command. To disable immediate-leave processing, use the **no** form of this command.

ip igmp snooping vlan *vlan_num* immediate-leave

no ip igmp snooping vlan *vlan_num* immediate-leave

Syntax Description	<i>vlan_num</i>	Number of the VLAN; valid values are from 1 to 4094.
	immediate-leave	Enables immediate leave processing.

Defaults Immediate leave processing is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended addressing was added.

Usage Guidelines You enter this command in global configuration mode only.

Use the immediate-leave feature only when there is a single receiver for the MAC group for a specific VLAN.

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 4:

```
Switch(config)# ip igmp snooping vlan 4 immediate-leave
Switch(config)#
```

This example shows how to disable IGMP immediate-leave processing on VLAN 4:

```
Switch(config)# no ip igmp snooping vlan 4 immediate-leave
Switch(config)#
```

Related Commands

- [ip igmp snooping](#)
- [ip igmp snooping vlan mrouter](#)
- [ip igmp snooping vlan static](#)
- [show ip igmp interface](#) (refer to Cisco IOS documentation)
- [show mac-address-table multicast](#)

ip igmp snooping vlan mrouter

To statically configure an Layer 2 interface as a multicast router interface for a VLAN, use the **ip igmp snooping vlan mrouter** command. To remove the configuration, use the **no** form of this command.

```
ip igmp snooping vlan vlan-id mrouter { interface { { FastEthernet slot/port } |
{ GigabitEthernet slot/port } | { port-channel number } } |
{ learn { cgmp | pim-dvmrp } }
```

```
no ip igmp snooping vlan vlan-id mrouter { interface { FastEthernet slot/port } |
{ GigabitEthernet slot/port } | { port-channel number } } |
{ learn { cgmp | pim-dvmrp } }
```

Syntax Description		
vlan <i>vlan-id</i>		Specifies the VLAN ID number to use in the command; valid values are from 1 to 4094.
interface		Specifies the next-hop interface to multicast switch.
FastEthernet		Specifies the Fast Ethernet interface.
<i>slot/port</i>		Number of the slot and port.
GigabitEthernet		Specifies the Gigabit Ethernet interface.
port-channel <i>number</i>		Port channel number; valid values are from 1 to 64.
learn		Specifies the multicast switch learning method.
cgmp		Specifies the multicast switch snooping CGMP packets.
pim-dvmrp		Specifies the multicast switch snooping PIM-DVMRP packets.

Defaults Multicast switch snooping PIM-DVMRP packets are specified.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended addressing was added.

Usage Guidelines You enter this command in VLAN interface configuration mode only.

The interface to the switch must be in the VLAN where you are entering the command. It must be both administratively up and line protocol up.

The CGMP learning method can decrease control traffic.

The learning method you configure is saved in NVRAM.

Static connections to multicast interfaces are supported only on switch interfaces.

Examples

This example shows how to specify the next-hop interface to multicast switch:

```
Switch(config-if)# ip igmp snooping 400 mrouter interface fastethernet 5/6
Switch(config-if)#
```

This example shows how to specify the multicast switch learning method:

```
Switch(config-if)# ip igmp snooping 400 mrouter learn cgmp
Switch(config-if)#
```

Related Commands

[ip igmp snooping](#)
[ip igmp snooping vlan immediate-leave](#)
[ip igmp snooping vlan static](#)
[show ip igmp snooping](#)
[show ip igmp snooping mrouter](#)

ip igmp snooping vlan static

To configure an Layer 2 interface as a member of a group, use the **ip igmp snooping vlan static** command. To remove the configuration, use the **no** form of this command.

```
ip igmp snooping vlan vlan_num static mac-address { interface { FastEthernet slot/port } |
  { GigabitEthernet slot/port } | { port-channel number } }
```

```
no ip igmp snooping vlan vlan_num static { { interface { FastEthernet slot/port } |
  { GigabitEthernet slot/port } | { port-channel number } }
```

Syntax Description		
vlan <i>vlan_num</i>		Number of the VLAN.
static <i>mac-address</i>		Group MAC address.
interface		Specifies the next-hop interface to multicast switch.
FastEthernet <i>slot/port</i>		Specifies the Fast Ethernet interface. Number of the slot and port.
GigabitEthernet <i>slot/port</i>		Specifies the Gigabit Ethernet interface. Number of the slot and port.
port-channel <i>number</i>		Port channel number; valid values are from 1 through 64.

Defaults This command has no default settings.

Command Modes Global configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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

```
Switch(config)# ip igmp snooping vlan 4 static 0100.5e02.0203 interface fastethernet 5/11
Configuring port FastEthernet5/11 on group 0100.5e02.0203 vlan 4
Switch(config)#
```

Related Commands

- [ip igmp snooping](#)
- [ip igmp snooping vlan immediate-leave](#)
- [ip igmp snooping vlan mrouter](#)
- [show mac-address-table multicast](#)

ip local-proxy-arp

To enable the local proxy ARP feature, use the **ip local-proxy-arp** command. To disable the local proxy ARP feature, use the **no** form of this command.

ip local-proxy-arp

no ip local-proxy-arp

Syntax Description This command has no arguments or keywords.

Defaults Local proxy ARP is disabled.

Command Modes Interface configuration

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Use this feature only on subnets where hosts are intentionally prevented from communicating directly to the switch on which they are connected.

ICMP redirect is disabled on interfaces where the local proxy ARP feature is enabled.

Examples This example shows how to enable the local proxy ARP feature:

```
Switch(config-if)# ip local-proxy-arp
Switch(config-if)#
```

ip mfib fastdrop

To enable MFIB fast drop, use the **ip mfib fastdrop** command. To disable MFIB fast drop, use the **no** form of this command.

ip mfib fastdrop

no ip mfib fastdrop

Syntax Description This command has no arguments or keywords.

Defaults MFIB fast drop is enabled.

Command Modes EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to enable MFIB fast drops:

```
Switch# ip mfib fastdrop
Switch#
```

Related Commands

- [clear ip mfib fastdrop](#)
- [show ip mfib fastdrop](#)

ip route-cache flow

To enable NetFlow statistics for IP routing, use the **ip route-cache flow** command. To disable NetFlow statistics, use the **no** form of this command.

ip route-cache flow [infer-fields]

no ip route-cache flow [infer-fields]

Syntax Description	infer-fields (Optional) Includes the NetFlow fields as inferred by the software: Input identifier, Output identifier, and Routing information.
---------------------------	---

Defaults	NetFlow statistics is disabled. Inferred information is excluded.
-----------------	--

Command Modes	Configuration
----------------------	---------------

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst4500 series switches.
	12.1(19)EW	Command enhanced to support infer fields.

Usage Guidelines	To use these commands, you need to install the Supervisor EngineIV and the NetFlow Service Card. The NetFlow statistics feature captures a set of traffic statistics. These traffic statistics include source IP address, destination IP address, layer 4 port information, protocol, input and output identifiers, and other routing information that can be used for network analysis, planning, accounting, billing and identifying DOS attacks.
-------------------------	--

NetFlow switching is supported on IP and IP-encapsulated traffic over all interface types.

If you enter **ip route-cache flow infer-fields** after **ip route-cache flow**, you will purge the existing cache, and vice versa. This is done to avoid having flows with and without inferred fields in the cache simultaneously.

For additional information on NetFlow switching, refer to the *Catalyst4500 Series Switch CiscoIOS Software Configuration Guide*.



Note

NetFlow consumes additional memory and CPU resources compared to other switching modes. You need to know the resources required on your switch before enabling NetFlow.

Examples

This example shows how to enable NetFlow switching on the switch:

```
Switch# config terminal
Switch(config)# ip route-cache flow
Switch(config)# exit
Switch#
```

**Note**

This command does not work on a per-interface basis.

ip source binding

To add or delete a static IP source binding entry, use the **ip source binding** command. Use the **no** form of this command to delete the corresponding IP source binding entry.

ip source binding *ip-address mac-address* **vlan** *vlan-id* **interface** *interface-name*

no ip source binding *ip-address mac-address* **vlan** *vlan-id* **interface** *interface-name*

Syntax Description		
	<i>ip-address</i>	Binding IP address.
	<i>mac-address</i>	Binding MAC address.
	vlan <i>vlan-id</i>	VLAN number.
	interface <i>interface-name</i>	Binding interface.

Defaults This command has no default settings.

Command Modes Global configuration

Command History	Release	Modification
	12.1(19)EW	This command was first introduced.

Usage Guidelines The **ip source binding** command is used to add a static IP source binding entry only. The **no** form of this command deletes the corresponding IP source binding entry. For the deletion to succeed, all required parameters must match. Each static IP binding entry is keyed by a MAC address and VLAN number. This implies that if the CLI contains an existing MAC and VLAN, the existing binding entry will be updated with the new parameters; a separate binding entry will not be created.

Examples This example shows how to configure the static IP source binding:

```
Switch# config terminal
Switch(config)# ip source binding 11.0.0.1 0000.000A.000B vlan 10 interface
fastethernet6/10
Switch(config)#
```

Related Commands [show ip source binding](#)

ip sticky-arp

To enable sticky ARP, use the **ip sticky-arp** command. 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 Enabled

Command Modes Global configuration

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines This command is supported on PVLANS only.

ARP entries that are learned on Layer3 PVLAN interfaces are sticky ARP entries. (You should display and verify ARP entries on the PVLAN interface using the **show arp** command).

For security reasons, sticky ARP entries on the PVLAN interface do not age out. Connecting new equipment with the same IP address generates a message and the ARP entry is not created.

Because the ARP entries on the PVLAN interface do not age out, you must manually remove ARP entries on the PVLAN interface if a MAC address changes.

Unlike static entries, sticky-ARP entries are not stored and restored when you enter the **reboot** and **restart** commands.

Examples This example shows how to enable sticky ARP:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) ip sticky-arp
Switch(config)# end
Switch#
```

This example shows how to disable sticky ARP:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) no ip sticky-arp
Switch(config)# end
Switch#
```

Related Commands **arp** (refer to Cisco IOS documentation)
 show arp (refer to Cisco IOS documentation)

ip verify header vlan all

To enable IP header validation for Layer 2-switched IPv4 packets, use the **ip verify header vlan all** command. To disable the IP header validation, use the **no** form of this command.

ip verify header vlan all

no ip verify header vlan all

Syntax Description This command has no default settings.

Defaults The IP header is validated for bridged and routed IPv4 packets.

Command Modes Configuration

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines This command does not apply to Layer 3-switched (routed) packets. The Catalyst 4500 series switch checks the validity of the following fields in the IPv4 header for all switched IPv4 packets:

- Version must be 4.
- Header length must be greater than or equal to 20 bytes.
- Total length must be greater than or equal to four times the header length, and greater than the Layer 2 packet size minus the Layer 2 encapsulation size.

If an IPv4 packet fails the IP header validation, the packet is dropped. If you disable header validation, packets with invalid IP headers are bridged but not routed even if routing was intended. IPv4 access lists also are not applied to IP headers.

Examples This example shows how to disable IP header validation for Layer 2-switched IPv4 packets:

```
Switch# config t
Switch(config)# no ip verify header vlan all
Switch(config)# end
Switch#
```

ip verify source vlan dhcp-snooping

To enable IP source guard on DHCP snooping untrusted Layer 2 interfaces, use the **ip verify source vlan dhcp-snooping** command. Use the **no** form of this command to disable IP source guard on DHCP snooping untrusted Layer 2 interfaces.

ip verify source vlan dhcp-snooping [port-security]

no ip verify source vlan dhcp-snooping [port-security]

Syntax Description	port-security (Optional) Filters both source IP and MAC addresses using the port security feature.				
Defaults	IP source guard is disabled.				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(19)EW</td> <td>Support for this command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Release	Modification				
12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.				
Usage Guidelines	Interface configuration				

Examples This example shows how to enable DHCP snooping security on VLANs 10 through 20:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10 20
Switch(config)# configure interface fastethernet6/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport access vlan 10
Switch(config-if)# no ip dhcp snooping trust
Switch(config-if)# ip verify source vlan dhcp-snooping
Switch(config)# end
Switch# show ip dhcp snooping security interface fastethernet6/1
Interface  Filter-type  Filter-mode  IP-address  Mac-address  Vlan
-----
fa6/1     ip           active       10.0.0.2    -----    10
fa6/1     ip           active       deny-all   -----    11-20
Switch#
```

The output shows that there is one valid DHCP binding to VLAN 10.

Related Commands

debug ip verify source packet (refer to Cisco IOS documentation)
ip dhcp snooping
ip dhcp snooping limit rate
ip dhcp snooping information option
ip dhcp snooping trust
ip source binding (refer to Cisco IOS documentation)
show ip dhcp snooping
show ip dhcp snooping binding
show ip verify source (refer to Cisco IOS documentation)
show ip source binding (refer to Cisco IOS documentation)

l2protocol-tunnel

To enable protocol tunneling on an interface, use the **l2protocol-tunnel** command. You can enable tunneling for Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunking Protocol (VTP) packets. Use the **no** form of this command to disable tunneling on the interface.

l2protocol-tunnel [**cdp** | **stp** | **vtp**]

no l2protocol-tunnel [**cdp** | **stp** | **vtp**]

Syntax Description

cdp	(Optional) Enables tunneling of CDP.
stp	(Optional) Enables tunneling of STP.
vtp	(Optional) Enables tunneling of VTP.

Defaults

The default is no Layer 2 protocol packets are tunneled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

You must enter this command, with or without protocol types, to tunnel Layer 2 packets.

Layer 2 protocol tunneling across a service-provider network ensures that Layer 2 information is propagated across the network to all customer locations. When protocol tunneling is enabled, protocol packets are encapsulated with a well known Cisco multicast address for transmission across the network. When the packets reach their destination, the well known MAC address is replaced by the Layer2 protocol MAC address.

You can enable Layer2 protocol tunneling for CDP, STP, and VTP individually or for all three protocols.

Examples

This example shows how to enable protocol tunneling for CDP packets:

```
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)#
```

Related Commands

[l2protocol-tunnel cos](#)
[l2protocol-tunnel drop-threshold](#)
[l2protocol-tunnel shutdown-threshold](#)

l2protocol-tunnel cos

To configure the class of service (CoS) value for all tunneled Layer 2 protocol packets, use the **l2protocol-tunnel cos** command. Use the **no** form of this command to return to the default value of zero.

l2protocol-tunnel cos *value*

no l2protocol-tunnel cos

Syntax Description	<i>value</i> Specifies the CoS priority value for tunneled Layer 2 protocol packets. 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	<table border="1"> <thead> <tr> <th style="border: none;">Release</th> <th style="border: none;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border: none;">12.2(18)EW</td> <td style="border: none;">This command was first introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)EW	This command was first introduced on the Catalyst 4500 series switch.
Release	Modification				
12.2(18)EW	This command was first introduced on the Catalyst 4500 series switch.				

Usage Guidelines	<p>When enabled, the tunneled Layer 2 protocol packets use this CoS value.</p> <p>The value is saved in NVRAM.</p>
-------------------------	--

Examples	<p>This example shows how to configure a Layer-2 protocol tunnel CoS value of 7:</p> <pre>Switch(config)# l2protocol-tunnel cos 7 Switch(config)#</pre>
-----------------	---

Related Commands	<p>l2protocol-tunnel</p> <p>l2protocol-tunnel drop-threshold</p> <p>l2protocol-tunnel shutdown-threshold</p>
-------------------------	--

l2protocol-tunnel drop-threshold

To set a drop threshold for the maximum rate of Layer2 protocol packets per second to be received before an interface drops packets, use the **l2protocol-tunnel drop-threshold** command. You can set the drop threshold for Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunking Protocol (VTP) packets. Use the **no** form of this command to disable the drop threshold on the interface.

l2protocol-tunnel drop-threshold [cdp | stp | vtp] value

no l2protocol-tunnel drop-threshold [cdp | stp | vtp] value

Syntax Description	
cdp	(Optional) Specifies a drop threshold for CDP.
stp	(Optional) Specifies a drop threshold for STP.
vtp	(Optional) Specifies a drop threshold for VTP.
<i>value</i>	Specifies a threshold in packets per second to be received for encapsulation before the interface shuts down, or specify the threshold before the interface drops packets. The range is 1 to 4096. The default is no threshold.

Defaults The default is no drop threshold for the number of Layer 2 protocol packets.

Command Modes Interface configuration

Command History	Release	Modification
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines 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.

Examples This example shows how to configure the drop threshold rate:

```
Switch(config-if)# l2protocol-tunnel drop-threshold cdp 50
Switch(config-if)#
```

Related Commands

- [l2protocol-tunnel](#)
- [l2protocol-tunnel cos](#)
- [l2protocol-tunnel shutdown-threshold](#)

l2protocol-tunnel shutdown-threshold

To configure the protocol tunneling encapsulation rate, use the **l2protocol-tunnel shutdown-threshold** command. You can set the encapsulation rate for Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunking Protocol (VTP) packets. Use the **no** form of this command to disable the encapsulation rate on the interface.

l2protocol-tunnel shutdown-threshold [**cdp** | **stp** | **vtp**] *value*

no l2protocol-tunnel shutdown-threshold [**cdp** | **stp** | **vtp**] *value*

Syntax Description

cdp	(Optional) Specifies a shutdown threshold for CDP.
stp	(Optional) Specifies a shutdown threshold for STP.
vtp	(Optional) Specifies a shutdown threshold for VTP.
<i>value</i>	Specifies a threshold in packets per second to be received for encapsulation before the interface shuts down. The range is 1 to 4096. The default is no threshold.

Defaults

The default is no shutdown threshold for the number of Layer 2 protocol packets.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Enter the **shutdown-threshold** keyword to control the number of protocol packets per second that are received on an interface before it shuts down. When no protocol option is specified with the keyword, the threshold is applied to each of the tunneled Layer 2 protocol types. If you also set a drop threshold on the interface, the shutdown-threshold value must be greater than or equal to the drop-threshold value.

When the shutdown threshold is reached, the interface is error disabled. If you enable error recovery by entering the **errdisable recovery cause l2ptguard** command, the interface is brought out of the error-disabled state and allowed to retry the operation again when all the causes have timed out. If the error recovery feature generation is not enabled for **l2ptguard**, the interface stays in the error-disabled state until you enter the **shutdown** and **no shutdown** commands.

Examples

This example shows how to configure the maximum rate:

```
Switch(config-if)# l2protocol-tunnel shutdown-threshold cdp 50
Switch(config-if)#
```

Related Commands

[l2protocol-tunnel](#)
[l2protocol-tunnel cos](#)
[l2protocol-tunnel shutdown-threshold](#)

lacp port-priority

To set the LACP priority for physical interfaces, use the **lacp port-priority** command.

lacp port-priority *priority*

Syntax Description	<i>priority</i> Priority for the physical interfaces; valid values are from 1 to 65535.
---------------------------	---

Defaults	Priority is set to 32768.
-----------------	---------------------------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	12.1(13)EW	This command was introduced on the Catalyst4500 series switches.

Usage Guidelines	<p>This command is not supported on systems configured with a Supervisor Engine 1.</p> <p>You must assign each port in the switch a port priority that can be specified automatically or by entering the lacp port-priority command. The port priority is used with the port number to form the port identifier. The port priority is used to decide which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.</p> <p>Although this command is a global configuration command, the <i>priority</i> value is supported only on port channels with LACP-enabled physical interfaces. This command is supported on LACP-enabled interfaces.</p> <p>When setting the priority, the higher the number, the lower the priority.</p>
-------------------------	---

Examples	This example shows how to set the priority for the interface:
-----------------	---

```
Switch(config-if)# lacp port-priority 23748
Switch(config-if)#
```

Related Commands	<p>channel-group</p> <p>channel-protocol</p> <p>lacp system-priority</p> <p>show lacp</p>
-------------------------	---

lacp system-priority

To set the priority of the system for LACP, use the **lacp system-priority** command.

lacp system-priority *priority*

Syntax Description	<i>priority</i>	Priority of the system; valid values are from 1 to 65535.
---------------------------	-----------------	---

Defaults	Priority is set to 32768.
-----------------	---------------------------

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

Command History	Release	Modification
	12.1(13)EW	This command was introduced on the Catalyst4500 series switches.

Usage Guidelines	<p>This command is not supported on systems configured with a Supervisor Engine 1.</p> <p>You must assign each switch running LACP a system priority that can be specified automatically or by entering the lacp system-priority command. The system priority is used with the switch MAC address to form the system ID and is also used during negotiation with other systems.</p> <p>Although this command is a global configuration command, the <i>priority</i> value is supported on port channels with LACP-enabled physical interfaces.</p> <p>When setting the priority, the higher the number, the lower the priority.</p> <p>You can also enter the lacp system-priority command in interface configuration mode. After you enter the command, the system defaults to global configuration mode.</p>
-------------------------	--

Examples	This example shows how to set the system priority:
-----------------	--

```
Switch(config)# lacp system-priority 23748
Switch(config)#
```

Related Commands	channel-group channel-protocol lacp port-priority show lacp
-------------------------	--

mac access-list extended

To define extended MAC access lists, use the **mac access-list extended** command. To remove MAC access lists, use the **no** form of this command.

mac access-list extended *name*

no mac access-list extended *name*

Syntax Description	<i>name</i> ACL to which the entry belongs.				
Defaults	MAC access lists are not defined.				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(12c)EW</td> <td>Support for this command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Release	Modification				
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.				

Usage Guidelines When you enter the ACL name, follow these naming conventions:

- Maximum of 31 characters long and can include a-z, A-Z, 0-9, the dash character (-), the underscore character (_), and the period character (.)
- Must start with an alpha character and must be unique across all ACLs of all types
- Case sensitive
- Cannot be a number
- Must not be a keyword; keywords to avoid are all, default-action, map, help, and editbuffer

When you enter the **mac access-list extended** *name* command, you use the **[no] {permit | deny} {{src-mac mask | any} [dest-mac mask]} [protocol-family {appletalk | arp-non-ipv4 | decnet | ipx | ipv6 | rarp-ipv4 | rarp-non-ipv4 | vines | xns}]** subset to create or delete entries in a MAC layer access list.

[Table2-7](#) describes the syntax of the **mac access-list extended** subcommands.

Table2-7 *mac access-list extended Subcommands*

Subcommand	Description
deny	Prevents access if the conditions are matched.
no	(Optional) Deletes a statement from an access list.
permit	Allows access if the conditions are matched.
<i>src-mac mask</i>	Source MAC address in the form: <i>source-mac-address source-mac-address-mask.</i>
any	Specifies any protocol type.

Table2-7 mac access-list extended Subcommands (continued)

Subcommand	Description
<i>dest-mac mask</i>	(Optional) Destination MAC address in the form: <i>dest-mac-address dest-mac-address-mask</i>
<i>protocol-family</i>	(Optional) Name of the protocol family. Table2-8 explains which packets are mapped to a particular protocol family.

[Table2-8](#) describes mapping an Ethernet packet to a protocol family.

Table2-8 Mapping an Ethernet Packet to a Protocol Family

Protocol Family	Ethertype in Packet Header
Appletalk	0x809B, 0x80F3
Arp-Non-Ipv4	0x0806 and protocol header of Arp is a non-Ip protocol family
Decnet	0x6000-0x6009, 0x8038-0x8042
Ipx	0x8137-0x8138
Ipv6	0x86DD
Rarp-Ipv4	0x8035 and protocol header of Rarp is Ipv4
Rarp-Non-Ipv4	0x8035 and protocol header of Rarp is a non-Ipv4 protocol family
Vines	0x0BAD, 0x0BAE, 0x0BAF
Xns	0x0600, 0x0807

When you enter the *src-mac mask* or *dest-mac mask* value, follow these guidelines:

- Enter MAC addresses as three 4-byte values in dotted hexadecimal format; for example, 0030.9629.9f84.
- Enter MAC address masks as three 4-byte values in dotted hexadecimal format. Use 1 bit as a wildcard. For example, to match an address exactly, use 0000.0000.0000 (can be entered as 0.0.0).
- For the optional *protocol* parameter, you can enter either the ethertype or the keyword.
- Entries without a *protocol* parameter match any protocol.
- Access lists entries are scanned in the order you enter them. The first matching entry is used. To improve performance, place the most commonly used entries near the beginning of the access list.
- An implicit **deny any any** entry exists at the end of an access list unless you include an explicit **permit any any** entry at the end of the list.
- All new entries to an existing list are placed at the end of the list. You cannot add entries to the middle of a list.

Examples

This example shows how to create a MAC layer access list named `mac_layer` that denies traffic from 0000.4700.0001, which is going to 0000.4700.0009, and permits all other traffic:

```
Switch(config)# mac access-list extended mac_layer
Switch(config-ext-macl)# deny 0000.4700.0001 0.0.0 0000.4700.0009 0.0.0 protocol-family appletalk
Switch(config-ext-macl)# permit any any
```

Related Commands [show vlan access-map](#)

mac-address-table aging-time

To configure aging time for entries in the Layer 2 table, use the **mac-address-table aging-time** command. To reset the *seconds* value to the default setting, use the **no** form of this command.

mac-address-table aging-time *seconds* [**vlan** *vlan_id*]

no mac-address-table aging-time *seconds* [**vlan** *vlan_id*]

Syntax Description	<i>seconds</i>	Aging time in seconds; valid values are 0 and from 10 to 1000000 seconds.
	vlan <i>vlan_id</i>	(Optional) Single VLAN number or a range of VLANs; valid values are from 1 to 4094.

Defaults Aging time is set to 300 seconds.

Command Modes Global configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended addressing was added.

Usage Guidelines If you do not enter a VLAN, the change is applied to all routed-port VLANs.
Enter 0 seconds to disable aging.

Examples This example shows how to configure the aging time to 400 seconds:

```
Switch(config)# mac-address-table aging-time 400
Switch(config)#
```

This example shows how to disable aging:

```
Switch(config)# mac-address-table aging-time 0
Switch(config)
```

Related Commands [show mac-address-table aging-time](#)

mac-address-table dynamic group protocols

To enable the learning of MAC addresses in both the “ip” and “other” protocol buckets, even though the incoming packet may belong to only one of the protocol buckets, use the **mac-address-table dynamic group protocols** command. To disable grouped learning, use the **no** form of this command.

mac-address-table dynamic group protocols { ip | other } { ip | other }

[no] mac-address-table dynamic group protocols { ip | other } { ip | other }

Syntax Description	ip	Specifies the “ip” protocol bucket.
	other	Specifies the “other” protocol bucket.

Defaults The group learning feature is disabled.

Command Modes global configuration

Command History	Release	Modification
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch..

Usage Guidelines The entries within the “ip” and “other” protocol buckets are created according to the protocol of the incoming traffic.

When you use the **mac-address-table dynamic group protocols** command, an incoming MAC address that might belong to either the “ip” or the “other” protocol bucket, is learned on both protocol buckets. Therefore, any traffic destined to this MAC address and belonging to any of the protocol buckets is unicast to that MAC address, rather than flooded. This reduces the unicast Layer 2 flooding that might be caused if the incoming traffic from a host belongs to a different protocol bucket than the traffic that is destined to the sending host.

Examples This example shows that the MAC addresses are initially assigned to either the “ip” or the “other” protocol bucket:

```
Switch# show mac-address-table dynamic
Unicast Entries
  vlan  mac address      type           protocols      port
-----+-----+-----+-----+-----
   1    0000.0000.5000    dynamic other           GigabitEthernet1/1
   1    0001.0234.6616    dynamic ip             GigabitEthernet3/1
   1    0003.3178.ec0a    dynamic assigned      GigabitEthernet3/1
   1    0003.4700.24c3    dynamic ip             GigabitEthernet3/1
   1    0003.4716.f475    dynamic ip             GigabitEthernet3/1
   1    0003.4748.75c5    dynamic ip             GigabitEthernet3/1
   1    0003.47f0.d6a3    dynamic ip             GigabitEthernet3/1
   1    0003.47f6.a91a    dynamic ip             GigabitEthernet3/1
```

mac-address-table dynamic group protocols

```

1    0003.ba06.4538    dynamic ip          GigabitEthernet3/1
1    0003.fd63.3eb4    dynamic ip          GigabitEthernet3/1
1    0004.2326.18a1    dynamic ip          GigabitEthernet3/1
1    0004.5a5d.de53    dynamic ip          GigabitEthernet3/1
1    0004.5a5e.6ecc    dynamic ip          GigabitEthernet3/1
1    0004.5a5e.f60e    dynamic ip          GigabitEthernet3/1
1    0004.5a5f.06f7    dynamic ip          GigabitEthernet3/1
1    0004.5a5f.072f    dynamic ip          GigabitEthernet3/1
1    0004.5a5f.08f6    dynamic ip          GigabitEthernet3/1
1    0004.5a5f.090b    dynamic ip          GigabitEthernet3/1
1    0004.5a88.b075    dynamic ip          GigabitEthernet3/1
1    0004.c1bd.1b40    dynamic ip          GigabitEthernet3/1
1    0004.c1d8.b3c0    dynamic ip          GigabitEthernet3/1
1    0004.c1d8.bd00    dynamic ip          GigabitEthernet3/1
1    0007.e997.74dd    dynamic ip          GigabitEthernet3/1
1    0007.e997.7e8f    dynamic ip          GigabitEthernet3/1
1    0007.e9ad.5e24    dynamic ip          GigabitEthernet3/1
1    000b.5f0a.f1d8    dynamic ip          GigabitEthernet3/1
1    000b.fdf3.c498    dynamic ip          GigabitEthernet3/1
1    0010.7be8.3794    dynamic assigned   GigabitEthernet3/1
1    0012.436f.c07f    dynamic ip          GigabitEthernet3/1
1    0050.0407.5fe1    dynamic ip          GigabitEthernet3/1
1    0050.6901.65af    dynamic ip          GigabitEthernet3/1
1    0050.da6c.81cb    dynamic ip          GigabitEthernet3/1
1    0050.dad0.af07    dynamic ip          GigabitEthernet3/1
1    00a0.ccd7.20ac    dynamic ip          GigabitEthernet3/1
1    00b0.64fd.1c23    dynamic ip          GigabitEthernet3/1
1    00b0.64fd.2d8f    dynamic assigned   GigabitEthernet3/1
1    00d0.b775.c8bc    dynamic ip          GigabitEthernet3/1
1    00d0.b79e.de1d    dynamic ip          GigabitEthernet3/1
1    00e0.4c79.1939    dynamic ip          GigabitEthernet3/1
1    00e0.4c7b.d765    dynamic ip          GigabitEthernet3/1
1    00e0.4c82.66b7    dynamic ip          GigabitEthernet3/1
1    00e0.4c8b.f83e    dynamic ip          GigabitEthernet3/1
1    00e0.4cbc.a04f    dynamic ip          GigabitEthernet3/1
1    0800.20cf.8977    dynamic ip          GigabitEthernet3/1
1    0800.20f2.82e5    dynamic ip          GigabitEthernet3/1
Switch#

```

This example shows how to assign MAC addresses that belong to either the “ip” or the “other” bucket to both buckets:

```

Switch(config)# mac-address-table dynamic group protocols ip other
Switch(config)# exit
Switch# show mac address-table dynamic
Unicast Entries
-----+-----+-----+-----+-----+
vlan  mac address      type      protocols      port
-----+-----+-----+-----+-----+
1      0000.0000.5000      dynamic  ip,other       GigabitEthernet1/1
1      0001.0234.6616      dynamic  ip,other       GigabitEthernet3/1
1      0003.4700.24c3      dynamic  ip,other       GigabitEthernet3/1
1      0003.4716.f475      dynamic  ip,other       GigabitEthernet3/1
1      0003.4748.75c5      dynamic  ip,other       GigabitEthernet3/1
1      0003.47c4.06c1      dynamic  ip,other       GigabitEthernet3/1
1      0003.47f0.d6a3      dynamic  ip,other       GigabitEthernet3/1
1      0003.47f6.a91a      dynamic  ip,other       GigabitEthernet3/1
1      0003.ba0e.24a1      dynamic  ip,other       GigabitEthernet3/1
1      0003.fd63.3eb4      dynamic  ip,other       GigabitEthernet3/1
1      0004.2326.18a1      dynamic  ip,other       GigabitEthernet3/1
1      0004.5a5d.de53      dynamic  ip,other       GigabitEthernet3/1
1      0004.5a5d.de55      dynamic  ip,other       GigabitEthernet3/1
1      0004.5a5e.6ecc      dynamic  ip,other       GigabitEthernet3/1
1      0004.5a5e.f60e      dynamic  ip,other       GigabitEthernet3/1
1      0004.5a5f.08f6      dynamic  ip,other       GigabitEthernet3/1

```



```

1      0004.5a5f.090b   dynamic ip,other      GigabitEthernet3/1
1      0004.5a64.f813   dynamic ip,other      GigabitEthernet3/1
1      0004.5a66.1a77   dynamic ip,other      GigabitEthernet3/1
1      0004.5a6b.56b2   dynamic ip,other      GigabitEthernet3/1
1      0004.5a6c.6a07   dynamic ip,other      GigabitEthernet3/1
1      0004.5a88.b075   dynamic ip,other      GigabitEthernet3/1
1      0004.c1bd.1b40   dynamic ip,other      GigabitEthernet3/1
1      0004.c1d8.b3c0   dynamic ip,other      GigabitEthernet3/1
1      0004.c1d8.bd00   dynamic ip,other      GigabitEthernet3/1
1      0005.dce0.7c0a   dynamic assigned      GigabitEthernet3/1
1      0007.e997.74dd   dynamic ip,other      GigabitEthernet3/1
1      0007.e997.7e8f   dynamic ip,other      GigabitEthernet3/1
1      0007.e9ad.5e24   dynamic ip,other      GigabitEthernet3/1
1      0007.e9c9.0bc9   dynamic ip,other      GigabitEthernet3/1
1      000b.5f0a.f1d8   dynamic ip,other      GigabitEthernet3/1
1      000b.fdf3.c498   dynamic ip,other      GigabitEthernet3/1
1      0012.436f.c07f   dynamic ip,other      GigabitEthernet3/1
1      0050.0407.5fe1   dynamic ip,other      GigabitEthernet3/1
1      0050.6901.65af   dynamic ip,other      GigabitEthernet3/1
1      0050.da6c.81cb   dynamic ip,other      GigabitEthernet3/1
1      0050.dad0.af07   dynamic ip,other      GigabitEthernet3/1
1      00a0.ccd7.20ac   dynamic ip,other      GigabitEthernet3/1
1      00b0.64fd.1b84   dynamic assigned      GigabitEthernet3/1
1      00d0.b775.c8bc   dynamic ip,other      GigabitEthernet3/1
1      00d0.b775.c8ee   dynamic ip,other      GigabitEthernet3/1
1      00d0.b79e.de1d   dynamic ip,other      GigabitEthernet3/1
1      00e0.4c79.1939   dynamic ip,other      GigabitEthernet3/1
1      00e0.4c7b.d765   dynamic ip,other      GigabitEthernet3/1
1      00e0.4c82.66b7   dynamic ip,other      GigabitEthernet3/1
1      00e0.4c8b.f83e   dynamic ip,other      GigabitEthernet3/1
1      00e0.4c8c.0861   dynamic ip,other      GigabitEthernet3/1
1      0800.20d1.bf09   dynamic ip,other      GigabitEthernet3/1
Switch#

```

Related Commands **mac-address-table dynamic** (refer to Cisco IOS documentation)

mac-address-table static

To configure static MAC addresses for a VLAN interface or drop unicast traffic for a MAC address for a VLAN interface, use the **mac-address-table static** command. To remove static MAC address configurations, use the **no** form of this command.

mac-address-table static *mac-addr* {**vlan** *vlan-id*} {**interface** *type* | **drop**}

no mac-address-table static *mac-addr* {**vlan** *vlan-id*} {**interface** *type*} {**drop**}

Syntax Description		
<i>mac-addr</i>	MAC address; optional when using the no form of the command.	
vlan <i>vlan-id</i>	VLAN and valid VLAN number; valid values are from 1 to 4094.	
interface <i>type</i>	Interface type and number; valid options are FastEthernet and GigabitEthernet .	
drop	Drops all traffic received from and going to the configured MAC address in the specified VLAN.	

Defaults This command has no default settings.

Command Modes Global configuration

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst4500 series switches.

Usage Guidelines

When a static MAC address is installed, it is associated with a port.

The output interface specified must be a Layer 2 interface and not an SVI.

If you do not enter a protocol type, an entry is automatically created for each of the four protocol types.

Entering the **no** form of this command does not remove system MAC addresses.

When removing a MAC address, entering **interface** *int* is optional. For unicast entries, the entry is removed automatically. For multicast entries, if you do not specify an interface, the entire entry is removed. You can specify the selected ports to be removed by specifying the interface.

Examples

This example shows how to add static entries to the MAC address table:

```
Switch(config)# mac-address-table static 0050.3e8d.6400 vlan 100 interface fastethernet5/7
Switch(config)#
```

This example shows how to configure a static MAC address with IGMP snooping disabled for a specified address:

```
Switch(config)# mac-address-table static 0050.3e8d.6400 vlan 100 interface fastethernet5/7 disable-snooping
Switch(config)#
```

Related Commands [show mac-address-table static](#)

macro apply cisco-desktop

To enable Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop, use the **macro apply cisco-desktop** command.

macro apply cisco-desktop \$AVID access_vlanid

Syntax Description	\$AVID access_vlanid Specifies an access VLAN ID.
---------------------------	--

Defaults	This command has no default settings.
-----------------	---------------------------------------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	<p>This command can only be viewed and applied; it cannot be modified.</p> <p>Ensure that the existing configuration on the interface does not conflict with the intended macro configuration. Before you apply the macro, clear the configuration on the interface with the default interface command.</p>
-------------------------	--

Examples	<p>This example shows how to enable the Cisco-recommended features and settings on port fa2/1:</p>
-----------------	--

```
Switch(config)# interface FastEthernet2/1
Switch(config-if)# macro apply cisco-desktop $AVID 50
Switch(config-if)#
```

This contents of this macro are as follows:

```
# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID [access_vlanid]
switchport mode access
# Enable port security limiting port to a single
# MAC address -- that of desktop
switchport port-security
# Ensure port-security age is greater than one minute
# and use inactivity timer
# "Port-security maximum 1" is the default and will not
# Show up in the config
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
```

Related Commands

macro apply cisco-phone
macro apply cisco-router
macro apply cisco-switch

macro apply cisco-phone

To enable Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop and a Cisco IP phone, use the **macro apply cisco-phone** command.

macro apply cisco-phone \$AVID *access_vlanid* \$VVID *voice_vlanid*

Syntax Description		
	\$AVID <i>access_vlanid</i>	Specifies an access VLAN ID.
	\$VVID <i>voice_vlanid</i>	Specifies a voice VLAN ID.

Defaults This command has no default settings.

Command Modes Interface configuration

Command History	Release	Modification
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines This command can only be viewed and applied; it cannot be modified.

Ensure that the existing configuration on the interface does not conflict with the intended macro configuration. Before you apply the macro, clear the configuration on the interface with the **default interface** command.

Examples This example shows how to enable the Cisco-recommended features and settings on port fa2/1:

```
Switch(config)# interface FastEthernet2/1
Switch(config-if)# macro apply cisco-phone $AVID 10 $VVID 50
Switch(config-if)#
```

This contents of this macro are as follows:

```
# VoIP enabled interface - Enable data VLAN
# and voice VLAN (VVID)
# Recommended value for access vlan (AVID) should not be 1\
switchport access vlan $AVID [access_vlan_id]
switchport mode access
# Update the Voice VLAN (VVID) value which should be
# different from data VLAN
# Recommended value for voice vlan (VVID) should not be 1
switchport voice vlan $VVID [voice_vlan_id]
# Enable port security limiting port to a 3 MAC
# addressees -- One for desktop and two for phone
switchport port-security
switchport port-security maximum 3
# 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
# Enable auto-qos to extend trust to attached Cisco phone
auto qos voip cisco-phone
# Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable@
```

Related Commands

[macro apply cisco-desktop](#)
[macro apply cisco-router](#)
[macro apply cisco-switch](#)

macro apply cisco-router

To enable Cisco-recommended features and settings that are suitable for connecting a switch port to a router, use the **macro apply cisco-router** command.

macro apply cisco-router *\$NVID native_vlanid*

Syntax Description	<i>\$NVID native_vlanid</i> Specifies a native VLAN ID.
---------------------------	---

Defaults	This command has no default settings.
-----------------	---------------------------------------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	<p>This command can only be viewed and applied; it cannot be modified.</p> <p>Ensure that the existing configuration on the interface does not conflict with the intended macro configuration. Before you apply macro apply cisco-router, clear the configuration on the interface with the default interface command.</p>
-------------------------	--

Examples	<p>This example shows how to enable the Cisco-recommended features and settings on port fa2/1:</p>
-----------------	--

```
Switch(config)# interface FastEthernet2/1
Switch(config-if)# macro apply cisco-router $NVID 80
Switch(config-if)#
```

This contents of this macro are as follows:

```
# Access Uplink to Distribution
switchport trunk encapsulation dot1q
# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (NVID) should not be 1
switchport trunk native vlan $NVID [native_vlan_id]
# Update the allowed VLAN range (VRANGE) such that it
# includes data, voice and native VLANs
# switchport trunk allowed vlan $VRANGE [vlan_range]
# Hardcode trunk and disable negotiation to
# speed up convergence
# Hardcode speed and duplex to router
switchport mode trunk
switchport nonegotiate
speed 100
duplex full
# Configure qos to trust this interface
auto qos voip trust
qos trust dscp
```



```
# Ensure fast access to the network when enabling the interface.  
# Ensure that switch devices cannot become active on the interface.  
spanning-tree portfast  
spanning-tree bpduguard enable
```

Related Commands**macro apply cisco-desktop****macro apply cisco-phone****macro apply cisco-switch**

macro apply cisco-switch

To enable Cisco-recommended features and settings that are suitable for connecting a switch port to another switch, use the **macro apply cisco-switch** command.

macro apply cisco-switch \$NVID *native_vlanid*

Syntax Description	\$NVID <i>native_vlanid</i> Specifies a native VLAN ID.
---------------------------	---

Defaults	This command has no default settings.
-----------------	---------------------------------------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	<p>This command can only be viewed and applied; it cannot be modified.</p> <p>Ensure that the existing configuration on the interface does not conflict with the intended macro configuration. Before you apply this macro, clear the configuration on the interface with the default interface command.</p>
-------------------------	---

Examples	<p>This example shows how to enable the Cisco-recommended features and settings on port fa2/1:</p>
-----------------	--

```
Switch(config)# interface FastEthernet2/1
Switch(config-if)# macro apply cisco-switch $NVID 45
Switch(config-if)#
```

This contents of this macro are as follows:

```
# Access Uplink to Distribution
switchport trunk encapsulation dot1q
# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (NVID) should not be 1
switchport trunk native vlan $NVID [native_vlan_id]
# Update the allowed VLAN range (VRANGE) such that it
# includes data, voice and native VLANs
# switchport trunk allowed vlan $VRANGE
# Hardcode trunk and disable negotiation to
# speed up convergence
switchport mode trunk
switchport nonegotiate
# Configure qos to trust this interface
auto qos voip trust
# 802.lw defines the link as pt-pt for rapid convergence
spanning-tree link-type point-to-point
```

Related Commands

[macro apply cisco-desktop](#)
[macro apply cisco-phone](#)
[macro apply cisco-router](#)

main-cpu

To enter the main CPU submode and manually synchronize the configurations on the two supervisor engines, use the **main-cpu** command.

main-cpu

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Redundancy

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch. (Catalyst 4507R only)

Usage Guidelines The main CPU submode is used to manually synchronize the configurations on the two supervisor engines.

From the main CPU submode, use the **auto-sync** command to enable automatic synchronization of the configuration files in NVRAM.



Note After you enter the main CPU submode, you can use the **auto-sync** command to automatically synchronize the configuration between the primary and secondary route processors based on the primary configuration. In addition, you can use all of the redundancy commands that are applicable to the main CPU.

Examples This example shows how to reenable the default automatic synchronization feature using the auto-sync standard command to synchronize the startup-config and config-register configuration of the active supervisor engine with the standby supervisor engine. Updates for the boot variables are automatic and cannot be disabled.

```
Switch(config)# redundancy
Switch(config-red)# main-cpu
Switch(config-r-mc)# auto-sync standard
Switch(config-r-mc)# end
Switch# copy running-config startup-config
Switch#
```

Related Commands [auto-sync](#)

match

To specify a match clause by selecting one or more ACLs for a VLAN access-map sequence, use the **match** subcommand. To remove the match clause, use the **no** form of this command.

```
match { ip address { acl-number | acl-name } } | { mac address acl-name }
```

```
no match { ip address { acl-number | acl-name } } | { mac address acl-name }
```



Note

If a match clause is not specified, the action for the VLAN access-map sequence is applied to all packets. All packets are matched against that sequence in the access-map.

Syntax Description

ip address <i>acl-number</i>	Selects one or more IP ACLs for a VLAN access-map sequence; valid values are from 1 to 199 and from 1300 to 2699.
ip address <i>acl-name</i>	Selects an IP ACL by name.
mac address <i>acl-name</i>	Selects one or more MAC ACLs for a VLAN access-map sequence.

Defaults

This command has no default settings.

Command Modes

VLAN access-map

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The match clause specifies the IP or MAC ACL for traffic filtering.

The MAC sequence is not effective for IP packets. IP packets should be access controlled by IP match clauses.

Refer to the *Catalyst4500 Series Switch CiscoIOS Software Configuration Guide* for additional configuration guidelines and restrictions.

Refer to the *Cisco IOS Command Reference* publication for additional **match** command information.

Examples

This example shows how to define a match clause for a VLAN access map:

```
Switch(config)# vlan access-map ganymede 10
Switch(config-access-map)# match ip address 13
Switch(config-access-map)#
```

Related Commands

[show vlan access-map](#)
[vlan access-map](#)

monitor session

To enable SPAN sessions on interfaces or VLANs, use the **monitor session** command. To remove one or more source or destination interfaces from a SPAN session, or a source VLAN from a SPAN session, use the **no** form of this command.

```
monitor session session {destination interface {FastEthernet interface-number |
GigabitEthernet interface-number} [encapsulation {isl | dot1q}] [ingress [vlan vlan_id]
[learning]]} | {remote vlan vlan_id} | {source {interface {FastEthernet interface-number |
GigabitEthernet interface-number | Port-channel interface-number} } | [vlan vlan_id]
| {remote vlan vlan_id} | {cpu [queue queue_id] [, | - | rx | tx | both]} | {filter {vlan vlan_id
[ , | - ]} | {packet-type {good | bad}} | {address-type {unicast | multicast | broadcast} [rx |
tx | both]}}
```

```
[no] monitor session session {destination interface {FastEthernet interface-number |
GigabitEthernet interface-number} [encapsulation {isl | dot1q}] [ingress [vlan vlan_id]
[learning]]} | {remote vlan vlan_id} | {source {interface {FastEthernet interface-number |
GigabitEthernet interface-number | Port-channel interface-number} } | [vlan vlan_id]
| {remote vlan vlan_id} | {cpu [queue queue_id] [, | - | rx | tx | both]} | {filter {vlan vlan_id
[ , | - ]} | {packet-type {good | bad}} | {address-type {unicast | multicast | broadcast} [rx |
tx | both]}}
```

Syntax Description

<i>session</i>	Number of a SPAN session; valid values are from 1 to 6.
destination	Specifies a SPAN destination.
interface	Specifies an interface.
FastEthernet <i>interface-number</i>	Specifies a Fast Ethernet module and port number; valid values are from 1 to 6.
GigabitEthernet <i>interface-number</i>	Specifies a Gigabit Ethernet module and port number; valid values are from 1 to 6.
encapsulation	(Optional) Specifies the encapsulation type of the destination port.
isl	(Optional) Specifies ISL encapsulation.
dot1q	(Optional) Specifies dot1q encapsulation.
ingress	(Optional) Indicates whether the ingress option is enabled.
vlan <i>vlan_id</i>	(Optional) Specifies the VLAN; valid values are from 1 to 4094.
learning	(Optional) Enables host learning on ingress-enabled destination ports.
remote vlan <i>vlan_id</i>	Specifies an RSPAN source or destination session on a switch.
source	Specifies a SPAN source.
Port-channel <i>interface-number</i>	Specifies a port channel interface; valid values are from 1 to 64.
cpu	Causes traffic received or sent from the CPU to be copied to the destination of the session.

queue <i>queue_id</i>	Specifies that only traffic received on the specific CPU subqueue should be copied to the destination of the session. Valid values are from 1 to 32, or by the following names: all, control-packet, rpf-failure, adj-same-if, nfl, mtu-exceeded, unknown-sa, span, acl input, acl input log, acl input error, acl input forward, acl input punt, acl output, acl output log, acl output error, acl output forward, acl output punt, bridged, bridged 1, bridged 2, bridged 3, bridged 4, routed received, routed received 1, routed received 2, routed received 3, routed received 4, routed forward, routed forward 1, routed forward 2, routed forward 3, and routed forward 4.
,	(Optional) Symbol to specify another range of SPAN VLANs; valid values are from 1 to 4094.
-	(Optional) Symbol to specify a range of SPAN VLANs.
both	(Optional) Monitors and filters received and transmitted traffic.
rx	(Optional) Monitors and filters received traffic only.
tx	(Optional) Monitors and filters transmitted traffic only.
filter	Limits SPAN source traffic to specific VLANs.
vlan <i>vlan_id</i>	(Optional) Specifies the VLAN to be filtered. The number is entered as a single value or a range; valid values are from 1 to 4094.
packet-type	Limits SPAN source traffic to packets of a specified type.
good	Specifies a good packet type
bad	Specifies a bad packet type.
address-type unicast multicast broadcast	Limits SPAN source traffic to packets of a specified address type. Valid types are unicast, multicast, and broadcast.

Defaults

Received and transmitted traffic, as well as all VLANs, packet types, and address types are monitored on a trunking interface.

Packets are transmitted untagged out the destination port; ingress and learning are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(11b)EW	Support for differing directions within a single-user session and extended VLAN addressing was added.
12.1(19)EW	Support for ingress packets, encapsulation specification, packet and address type filtering, and CPU source sniffing enhancements.
12.1(20)EW	Support for remote SPAN and host learning on ingress-enabled destination ports was added.

Usage Guidelines

Only one SPAN destination for a SPAN session is supported. If you attempt to add another destination interface to a session that already has a destination interface configured, you will get an error. You must first remove a SPAN destination interface before changing the SPAN destination to a different interface.

With release 12.1(12c)EW, you can configure sources from different directions within a single user session.



Note With release 12.1(12c)EW, SPAN is limited to two sessions containing ingress sources and four sessions containing egress sources. Bidirectional sources support both ingress and egress sources.

A particular SPAN session can either monitor VLANs or monitor individual interfaces: you cannot have a SPAN session that monitors both specific interfaces and specific VLANs. If you first configure a SPAN session with a source interface, and then try to add a source VLAN to the same SPAN session, you will receive an error. You will also receive an error message if you configure a SPAN session with a source VLAN, and then try to add a source interface to that session. You must first clear any sources for a SPAN session before switching to another type of source. CPU sources may be combined with source interfaces and source VLANs.

When configuring the **ingress** option on a destination port, you must specify an ingress VLAN if the configured encapsulation type is untagged (the default) or is 802.1q. If the encapsulation type is ISL, then no ingress VLAN specification is necessary.

By default, when you enable ingress, no host learning is performed on destination ports. When you enter the **learning** keyword, host learning is performed on the destination port, and traffic to learned hosts is forwarded out the destination port.

If you enter the **filter** keyword on a monitored trunking interface, only traffic on the set of specified VLANs is monitored. Port channel interfaces are displayed in the list of **interface** options if you have them configured. VLAN interfaces are not supported. However, you can span a particular VLAN by entering the **monitor session session source vlan vlan-id** command.

Packet-type filters are only supported in the RX direction. You can specify both Rx- and Tx-type filters as well as multiple-type filters at the same time (for example, you can use **good** and **unicast** to only sniff no error unicast frames). As with VLAN filters, if you do not specify the type, then the session will sniff all packet types.

The **queue** identifier allows sniffing for only traffic sent or received on the specified CPU queues. Queues may be identified either by number or by name. Queue names may contain multiple numbered queues for convenience.

Examples

This example shows how to add a source interface to a SPAN session:

```
Switch(config)# monitor session 1 source interface fa2/3
Switch(config)#
```

This example shows how to configure sources with different directions within a SPAN session:

```
Switch(config)# monitor session 1 source interface fa2/3 rx
Switch(config)# monitor session 1 source interface fa2/2 tx
Switch(config)#
```

This example shows how to remove a source interface from a SPAN session:

```
Switch(config)# no monitor session 1 source interface fa2/3
Switch(config)#
```


This example shows how to limit SPAN traffic to VLANs 100 through 304:

```
Switch(config)# monitor session 1 filter vlan 100 - 304  
Switch(config)#
```

This example shows how to configure RSPAN VLAN 20 as the destination:

```
Switch(config)# monitor session 2 destination remote vlan 20  
Switch(config)#
```

Related Commands [show monitor](#)

mtu

To enable jumbo frames on an interface by adjusting the maximum size of a packet, or maximum transmission unit (MTU), use the **mtu** command. To return to the default setting, use the **no** form of this command.

mtu *bytes*

no mtu

Syntax Description	<i>bytes</i>	Byte size; valid values are from 1500 to 9198.
---------------------------	--------------	--

Defaults	The default settings are as follows:
-----------------	--------------------------------------

- Jumbo frames are disabled
- 1500 bytes for all ports

Command Modes	Interface configuration mode
----------------------	------------------------------

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst4500 series switches.

Usage Guidelines	Jumbo frames are supported on non-blocking Gigabit Ethernet ports, switch virtual interfaces (SVI), and EtherChannels. Jumbo frames are not available for stub-based ports.
-------------------------	---

The baby giants feature uses the global **system mtu size** command to set the global baby giant MTU. It allows all stub-based ports interfaces to support Ethernet payload size of up to 1552 bytes.

Both the **system mtu** command and the per-interface **mtu** command work on interfaces that can support jumbo frames, but the per-interface **mtu** command takes precedence.

Examples	This example shows how to specify an MTU of 1800 bytes:
-----------------	---

```
Switch(config)# interface GigabitEthernet 1/1
Switch(config-if)# mtu 1800
```

Related Commands	system mtu
-------------------------	----------------------------

name

To set the MST region name, use the **name** command. To return to the default name, use the **no** form of this command.

name *name*

no name *name*

Syntax Description	<i>name</i>	Specifies the name of the MST region. The name can be any string with a maximum length of 32 characters.
--------------------	-------------	--

Defaults	The MST region name is not set.
----------	---------------------------------

Command Modes	MST configuration
---------------	-------------------

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	Two or more Catalyst 4500 series switches with the same VLAN mapping and configuration version number are considered to be in different MST regions if the region names are different.
------------------	--

Examples	This example shows how to name a region:
----------	--

```
Switch(config-mst)# name Cisco
Switch(config-mst)#
```

Related Commands	instance revision show spanning-tree mst spanning-tree mst configuration
------------------	---

pagp learn-method

To learn the input interface of incoming packets, use the **pagp learn-method** command. To return to the default value, use the **no** form of this command.

pagp learn-method { aggregation-port | physical-port }

no pagp learn-method

Syntax Description	aggregation-port	Specifies learning the address on the port channel.
	physical-port	Specifies learning the address on the physical port within the bundle.

Defaults Aggregation port is enabled.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to enable port channel address learning:

```
Switch(config-if)# pagp learn-method
Switch(config-if)#
```

This example shows how to enable physical port address learning within the bundle:

```
Switch(config-if)# pagp learn-method physical-port
Switch(config-if)#
```

This example shows how to enable aggregation port address learning within the bundle:

```
Switch(config-if)# pagp learn-method aggregation-port
Switch(config-if)#
```

Related Commands [pagp learn-method](#)
[show pagp](#)

pagp port-priority

To select a port in hot standby mode, use the **pagp port-priority** command. To return to the default value, use the **no** form of this command.

pagp port-priority *priority*

no pagp port-priority

Syntax Description	<i>priority</i> Port priority number; valid values are from 1 to 255.
---------------------------	---

Defaults	Port priority is set to 128.
-----------------	------------------------------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	The higher the priority, the better the chances are that the port will be selected in the hot standby mode.
-------------------------	---

Examples	This example shows how to set the port priority:
-----------------	--

```
Switch(config-if)# pagp port-priority 45
Switch(config-if)#
```

Related Commands	pagp learn-method show pagp
-------------------------	--

permit

To permit an ARP packet based on matches against the DHCP bindings, use the **permit** command. Use the **no** form of the command to remove specified ACEs from the access 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	Specifies the sender IP address.
any	Specifies that any IP or MAC address will be accepted.
host <i>sender-ip</i>	Specifies that only a specific sender IP address will be accepted.
<i>sender-ip</i> <i>sender-ip-mask</i>	Specifies that a specific range of sender IP addresses will be accepted.
mac	Specifies the sender MAC address.
host <i>sender-mac</i>	Specifies that only a specific sender MAC address will be accepted.
<i>sender-mac</i> <i>sender-mac-mask</i>	Specifies that a specific range of sender MAC addresses will be accepted.
response	Specifies a match for the ARP responses.
ip	Specifies the IP address values for the ARP responses.
host <i>target-ip</i>	(Optional) Specifies that only a specific target IP address will be accepted.
<i>target-ip target-ip-mask</i>	(Optional) Specifies that a specific range of target IP addresses will be accepted.
mac	Specifies the MAC address values for the ARP responses.
host <i>target-mac</i>	(Optional) Specifies that only a specific target MAC address will be accepted.
<i>target-mac</i> <i>target-mac-mask</i>	(Optional) Specifies that a specific range of target MAC addresses will be accepted.
log	(Optional) Logs a packet when it matches the access control entry (ACE).

Defaults

This command has no default settings.

Command Modes

arp-nacl configuration

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Permit clauses can be added to forward or drop ARP packets based on some matching criteria.

Examples A host with a MAC address of 0000.0000.abcd has an IP address of 1.1.1.1. To permit both requests and responses from this host, define an access list as follows:

```
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
Switch# show arp access-list

ARP access list static-hosts
    permit ip host 1.1.1.1 mac host 0000.0000.abcd
Switch#
```

Related Commands

- [arp access-list](#)
- [deny](#)
- [ip arp inspection filter vlan](#)

policy-map

To access the QoS policy map configuration mode to configure the QoS policy map, use the **policy-map** command. To delete a policy map, use the **no** form of this command.

policy-map *policy-map-name*

no policy-map *policy-map-name*

Syntax Description

policy-map-name Specifies the name of the policy map.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

In QoS policy-map configuration mode, these configuration commands are available:

- **exit** exits QoS class map configuration mode.
- **no** removes an existing defined policy map.
- **class** *class-map-name* accesses the QoS class map configuration mode to specify a previously created class map to be included in the policy map or to create a class map. (See the [class-map](#) command for additional information.)
- **police** [**aggregate** *name*] *rate burst* [**conform-action** {**drop** | **transmit**}] [{**exceed-action** {**drop** | **policed-dscp-transmit** | **transmit**}] defines a microflow or aggregate policer.
- **trust** {**cos** | **dscp**} sets the specified class trust values. Trust values that are set in this command supersede trust values set on specific interfaces.

Examples

This example shows how to create a policy map named **ipp5-policy** that uses the class-map named **ipp5** and is configured to rewrite the packet precedence to 6 and to aggregate police the traffic that matches IP precedence value of 5:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map ipp5-policy
Switch(config-pmap)# class ipp5
Switch(config-pmap-c)# set ip precedence 6
Switch(config-pmap-c)# police 2000000000 2000000 conform-action transmit exceed-action
policed-dscp-transmit
Switch(config-pmap-c)# end
```

Related Commands

[class-map](#)
[service-policy](#)
[show class-map](#)
[show policy-map](#)
[show policy-map interface](#)

port-channel load-balance

To set the load distribution method among the ports in the bundle, use the **port-channel load-balance** command. To reset the load distribution to the default, use the **no** form of this command.

port-channel load-balance *method*

no port-channel load-balance

Syntax Description	<i>method</i> Specifies the load distribution method. See “Usage Guidelines” for more information.
---------------------------	--

Defaults	Load distribution on the source XOR destination IP address is enabled.
-----------------	--

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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	<p>The following values are valid for the load distribution <i>method</i>:</p> <ul style="list-style-type: none"> • dst-ip—Load distribution on the destination IP address • dst-mac—Load distribution on the destination MAC address • dst-port—Load distribution on the destination TCP/UDP port • src-dst-ip—Load distribution on the source XOR destination IP address • src-dst-mac—Load distribution on the source XOR destination MAC address • src-dst-port—Load distribution on the source XOR destination TCP/UDP port • src-ip—Load distribution on the source IP address • src-mac—Load distribution on the source MAC address • src-port—Load distribution on the source port
-------------------------	--

Examples	This example shows how to set the load distribution method to destination IP address:
-----------------	---

```
Switch(config)# port-channel load-balance dst-ip
Switch(config)#
```

This example shows how to set the load distribution method to source XOR destination IP address:

```
Switch(config)# port-channel load-balance src-dst-port
Switch(config)#
```

Related Commands [interface port-channel](#)
[show etherchannel](#)

power dc input

To configure power DC input parameters on the switch, use the **power dc input** command. To return to the default power settings, use the **no** form of this command.

power dc input *watts*

no power dc input

Syntax Description	Command	Description
	dc input	Specifies the external DC source for both power supply slots.
	<i>watts</i>	Sets the total capacity of the external DC source in watts; valid values are from 300 to 8500.

Defaults DC power input is 2500 watts.

Command Modes Global configuration

Command History	Release	Modification
	12.1(11)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(13)EW	Support for dc input was added.

Usage Guidelines If your interface is not capable of supporting Power over Ethernet, you will receive the following error message:

```
Power over Ethernet not supported on interface Admin
```

Examples This example shows how to set the total capacity of the external DC power source to 5000 watts:

```
Switch(config)# power dc input 5000
Switch(config)#
```

Related Commands [show power](#)

power inline

To set the inline-power state for the inline-power-capable interfaces, use the **power inline** command. To return to the default values, use the **no** form of this command.

```
power inline { auto [max milliwatt] | never | static [max milliwatt] | consumption milliwatt }
no power inline
```

Syntax Description	auto	Sets the Power over Ethernet state to auto mode for inline-power-capable interfaces.
	max milliwatt	(Optional) Maximum power that the equipment can consume; valid range is from 2000 to 15400 mW.
	never	Disables both the detection and power for the inline-power capable interfaces.
	static	Allocates power statically.
	consumption milliwatt	Sets power allocation per interface; valid range is from 4000 to 15400. Any non-default value disables automatic adjustment of power allocation.

Defaults

The default settings are as follows:

- Auto mode for Power over Ethernet is set.
- Maximum milliwatt mode is set to 15400.
- Default allocation is set to 15400.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(19)EW	Support added for static power allocation.
12.1(20)EW	Support added for Power over Ethernet.

Usage Guidelines

If your interface is not capable of supporting Power over Ethernet, you will receive this message:

```
Power over Ethernet not supported on interface Admin
```

Examples

This example shows how to set the inline-power detection and power for the inline-power-capable interfaces:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 4/1
Switch(config-if)# power inline auto
Switch(config-if)# end
Switch#
```

This example shows how to disable the inline-power detection and power for the inline-power-capable interfaces:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 4/1
Switch(config-if)# power inline never
Switch(config-if)# end
Switch#
```

This example shows how to set the permanent Power over Ethernet allocation to 8000 mW for Fast Ethernet interface 4/1 regardless what is mandated either by the 802.3af class of the discovered device or by any CDP packet that is received from the powered device:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 4/1
Switch(config-if)# power inline consumption 8000
Switch(config-if)# end
Switch#
```

Related Commands

[power inline consumption](#)
[show power](#)

power inline consumption

To set the default power that is allocated to an interface for all the inline-power-capable interfaces on the switch, use the **power inline consumption** command. To return to the default values, use the **no** form of this command.

power inline consumption default *milliwatts*

no power inline consumption default

Syntax Description	default	Specifies the switch to use the default allocation.
	<i>milliwatts</i>	Sets the default power allocation in milliwatts; the valid range is from 4000 to 15400. Any non-default value disables automatic adjustment of power allocation.

Defaults Milliwatt mode is set to 15400.

Command Modes Global configuration

Command History	Release	Modification
	12.1(11)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(20)EW	Support added for Power over Ethernet.

Usage Guidelines If your interface is not capable of supporting Power over Ethernet, you will receive this message:

```
Power over Ethernet not supported on interface Admin
```

Examples This example shows how to set the Power over Ethernet allocation to use 8000 mW, regardless of any CDP packet that is received from the powered device:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# power inline consumption default 8000
Switch(config)# end
Switch#
```

Related Commands [power inline](#)
[show power](#)

power redundancy-mode

To configure the power settings for the chassis, use the **power redundancy-mode** command. To return to the default setting, use the **default** form of this command.

power redundancy-mode {redundant | combined}

default power redundancy-mode

Syntax Description	Command	Description
	redundant	Configures the switch to redundant power management mode.
	combined	Configures the switch to combined power management mode.

Defaults Redundant power management mode

Command Modes Global configuration

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch. (Catalyst4500 series switches only: 4503, 4506, and 4507)

Usage Guidelines The two power supplies must be the same type and wattage.



Caution

If you have power supplies with different types or wattages installed in your switch, the switch will not recognize one of the power supplies. A switch set to redundant mode will not have power redundancy. A switch set to combined mode will only use one power supply.

In redundant mode, the power from a single power supply must provide enough power to support the switch configuration.

[Table2-9](#) lists the maximum available power for chassis and Power over Ethernet for each power supply.

Table2-9 Available Power

Power Supply	Redundant Mode (W)	Combined Mode (W)
1000 W AC	System ¹ = 1000 Inline = 0	System = 1667 Inline = 0
2800 W AC	System = 1360 Inline = 1400	System = 2473 Inline = 2333

1. System power includes power for the supervisor engines, all line cards and the fan tray.

Examples

This example shows how to set the power management mode to combined:

```
Switch(config)# power redundancy-mode combined
Switch(config)#
```

Related Commands

[show power](#)

power supplies required

To configure the power redundancy mode for the Catalyst 4006 (only), use the **power supplies required** command. To return to the default power redundancy mode, use the **default** form of this command or the **power supplies required 2** command.

power supplies required {1 | 2}

default power supplies required

Syntax Description	1	Configures the chassis for 1+1 redundancy mode.
	2	Configures the switch to 2+1 redundancy mode.

Defaults 2+1 redundancy mode

Command Modes Global configuration

Command History	Release	Modification
	12.1(11)EW	Support for this command was introduced on the Catalyst 4500 series switch (Catalyst 4006 only).

Usage Guidelines This command is not supported on a Catalyst4500 series switch.

Examples This example shows how to set the power supplies required for the chassis to 1:

```
Switch(config)# power supplies required 1
Switch(config)#
```

Related Commands [show power](#)

private-vlan

To configure PVLANS and the association between a PVLAN and a secondary VLAN, use the **private-vlan** commands. To return to the default value, use the **no** form of this command.

private-vlan { **isolated** | **primary** }

private-vlan association *secondary-vlan-list* [{ **add** *secondary-vlan-list* } | { **remove** *secondary-vlan-list* }]

no private-vlan { **isolated** | **primary** }

no private-vlan association

Syntax Description		
isolated		Designates the VLAN as an isolated PVLAN.
primary		Designates the VLAN as the primary PVLAN.
association		Creates an association between a secondary VLAN and a primary VLAN.
<i>secondary-vlan-list</i>		Specifies the number of the secondary VLAN.
add		Associates a secondary VLAN to a primary VLAN.
remove		Clears the association between a secondary VLAN and a primary VLAN.

Defaults Private VLANs are not configured.

Command Modes VLAN configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended addressing was added.

Usage Guidelines You cannot configure VLAN 1 or VLANs 1001 to 1005 as PVLANS.

VTP does not support private VLANs. You must configure private VLANs on each device where you want private VLAN ports.

The *secondary_vlan_list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single PVLAN ID or a range of PVLAN IDs separated by hyphens.

The *secondary_vlan_list* parameter can contain multiple community VLAN IDs.

The *secondary_vlan_list* parameter can contain only one isolated VLAN ID. A PVLAN is defined as a set of private ports characterized by a common set of VLAN number pairs: each pair is made up of at least two special unidirectional VLANs and is used by isolated ports and/or by a community of ports to communicate with switches.

An isolated VLAN is a VLAN used by isolated ports to communicate with promiscuous ports. The isolated VLAN traffic is blocked on all other private ports in the same VLAN and can be received only by standard trunking ports and promiscuous ports assigned to the corresponding primary VLAN.

A promiscuous port is a private port assigned to a primary VLAN.

A primary VLAN is a VLAN used to convey the traffic from the switches to customer end stations on private ports.

You can specify only one isolated *vlan-id* value, while multiple community VLANs are allowed. You can only associate isolated and community VLANs to one VLAN. The associated VLAN list may not contain primary VLANs. Similarly, a VLAN already associated to a primary VLAN cannot be configured as a primary VLAN.

The **private-vlan** commands do not take effect until you exit the config-VLAN submode.

If you delete either the primary or secondary VLAN, the ports associated with the VLAN become inactive.

Refer to the *Catalyst4500 Series Switch CiscoIOS Software Configuration Guide* for additional configuration guidelines.

Examples

This example shows how to create a PVLAN relationship among the primary VLAN 14, the isolated VLAN 19, and community VLANs 20 and 21:

```
Switch(config)# vlan 19
Switch(config-vlan) # private-vlan isolated
Switch(config)# vlan 14
Switch(config-vlan) # private-vlan primary
Switch(config-vlan) # private-vlan association 19
```

This example shows how to remove an isolated VLAN from the PVLAN association:

```
Switch(config)# vlan 14
Switch(config-vlan) # private-vlan association remove 18
Switch(config-vlan)#
```

This example shows how to remove a PVLAN relationship and deletes the primary VLAN. The associated secondary VLANs are not deleted.

```
Switch(config-vlan) # no private-vlan 14
Switch(config-vlan)#
```

Related Commands

[show vlan](#)
[show vlan private-vlan](#)

private-vlan mapping

To create a mapping between the primary and the secondary VLANs, so that both share the same primary VLAN SVI, use the **private-vlan mapping** command. To remove all PVLAN mappings from an SVI, use the **no** form of the command.

```
private-vlan mapping primary-vlan-id {[secondary-vlan-list | {add secondary-vlan-list} |
{remove secondary-vlan-list}]}
```

```
no private-vlan mapping
```

Syntax Description

<i>primary-vlan-id</i>	VLAN ID of the primary VLAN of the PVLAN relationship.
<i>secondary-vlan-list</i>	(Optional) VLAN ID of the secondary VLANs to map to the primary VLAN.
add	(Optional) Maps the secondary VLAN to the primary VLAN.
remove	(Optional) Removes the mapping between the secondary VLAN and the primary VLAN.

Defaults

All PVLAN mappings are removed.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The *secondary_vlan_list* parameter cannot contain spaces. It can contain multiple, comma-separated items. Each item can be a single PVLAN ID or a range of PVLAN IDs separated by hyphens.

This command is valid in the interface configuration mode of the primary VLAN.

The SVI of the primary VLAN is created at Layer 3.

Traffic received on the secondary VLAN is routed by the SVI of the primary VLAN.

The SVIs of existing secondary VLANs do not function and are considered down after this command is entered.

A secondary SVI can be mapped to only one primary SVI. If the configured PVLANS association is different from what is specified in this command, for example if the specified *primary-vlan-id* is configured as a secondary VLAN, all the SVIs specified in this command are brought down.

If you configure a mapping between two VLANs that do not have a valid Layer 2 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(config)# interface vlan 18
Switch(config-if)# private-vlan mapping 18 20
Switch(config-if)#
```

This example shows how to permit routing of secondary VLAN ingress traffic from PVLANS 303 through 307, 309, and 440 and how to verify the configuration:

```
Switch# config terminal
Switch(config)# interface vlan 202
Switch(config-if)# private-vlan mapping add 303-307,309,440
Switch(config-if)# end
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type
-----
vlan202 303 isolated
vlan202 304 isolated
vlan202 305 isolated
vlan202 306 isolated
vlan202 307 isolated
vlan202 309 isolated
vlan202 440 isolated
Switch#
```

This example shows the displayed error message you will see if the VLAN you are adding is already mapped to the SVI of VLAN 18. You must delete the mapping from the SVI of VLAN 18 first:

```
Switch(config)# interface vlan 19
Switch(config-if)# private-vlan mapping 19 add 21
Command rejected: The interface for VLAN 21 is already mapped as s secondary.
Switch(config-if)#
```

This example shows how to remove all PVLAN mappings from the SVI of VLAN 19:

```
Switch(config)# interface vlan 19
Switch(config-if)# no private-vlan mapping
Switch(config-if)#
```

Related Commands

[show interfaces private-vlan mapping](#)
[show vlan](#)
[show vlan private-vlan](#)

private-vlan synchronize

To map secondary VLANs to the same instance as the primary VLAN, use the **private-vlan synchronize** command.

private-vlan synchronize

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes MST configuration

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines If you do not map VLANs to the same instance as the associated primary VLAN when you exit the MST configuration submode, a warning message displays and lists the secondary VLANs that are not mapped to the same instance as the associated primary VLAN. The **private-vlan synchronize** command automatically maps all secondary VLANs to the same instance as the associated primary VLANs.

Examples This example shows how to initialize PVLAN synchronization:

```
Switch(config-mst)# private-vlan synchronize
Switch(config-mst)#
```

This example assumes that a primary VLAN 2 and a secondary VLAN 3 are associated to VLAN 2, and that all VLANs are mapped to the CIST instance 1. This example also shows the output if you try to change the mapping for the primary VLAN 2 only:

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 2
Switch(config-mst)# exit
These secondary vlans are not mapped to the same instance as their primary:
->3
Switch(config)#
```

Related Commands [show spanning-tree mst](#)

qos (global configuration mode)

To globally enable QoS functionality on the switch, use the **qos** command. To globally disable QoS functionality, use the **no** form of this command.

qos

no qos

Syntax Description This command has no arguments or keywords.

Defaults QoS functionality is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines If QoS functionality is globally enabled, it is enabled on all interfaces, except on the interfaces where QoS has been disabled. If QoS functionality is globally disabled, all traffic is passed in QoS pass-through mode.

Examples This example shows how to enable QoS functionality globally on the switch:

```
Switch(config)# qos
Switch(config)#
```

Related Commands [qos \(interface configuration mode\)](#)
[show qos](#)

qos (interface configuration mode)

To enable QoS functionality on an interface, use the **qos** command. To disable QoS functionality on an interface, use the **no** form of this command.

qos

no qos

Syntax Description This command has no arguments or keywords.

Defaults QoS is enabled.

Command Modes Interface configuration

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines If QoS functionality is globally disabled, it is also disabled on all interfaces.

Examples This example shows how to enable QoS functionality on an interface:

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

Related Commands [show qos](#)
[qos \(global configuration mode\)](#)

qos account layer2 encapsulation

To include additional bytes to be accounted by QoS features, use the **qos account layer2 encapsulation** command. Use the **no** form of this command to disable the use of additional bytes.

```
qos account layer2 encapsulation { arpa | dot1q | isl | length len }
```

```
no qos account layer2 encapsulation { arpa | dot1q | isl | length len }
```

Syntax Description

arpa	Account length of the Ethernet ARPA encapsulated packet (18 bytes).
dot1q	Account length of the IEEE 802.1q encapsulated packet (22 bytes).
isl	Account length of the ISL encapsulated packet (48 bytes).
length len	Additional packet length to account for; valid range is from 0 to 64 bytes.

Defaults

By default, only the length specified in the IP header for IP packets and the length specified in the Ethernet header for non-IP packets is included.

Command Modes

Global configuration

Command History

Release	Modification
12.1(19)EW	This command was first introduced.

Usage Guidelines

In the Catalyst 4500 series switch, the **qos account layer2 encapsulation** command indicates that the policing feature should consider the configured length in addition to the IP length of the packet when policing IP packets.

Sharing and shaping always use the Ethernet ARPA length.



Note

The given length is included when policing all IP packets irrespective of the encapsulation with which it was received. When **qos account layer2 encapsulation isl** is configured, a fixed length of 48 bytes is included when policing all IP packets, not only those IP packets received with ISL encapsulation.

Sharing and shaping use the length specified in the Layer 2 headers.

Examples

This example shows how to include an additional 18 bytes when policing IP packets:

```
Switch# config terminal
Switch(conf)# qos account layer2 encapsulation length 18
Switch (conf)#
```

This example shows how to disable consistent accounting of Layer 2 encapsulation by QoS features:

```
Switch# config terminal  
Switch(conf)# no qos account layer2 encapsulation  
Switch (conf)#
```

Related Commands

[show interfaces
switchport
switchport block](#)

qos aggregate-policer

To define a named aggregate policer, use the **qos aggregate-policer** command. To delete a named aggregate policer, use the **no** form of this command.

```
qos aggregate-policer name rate burst [conform-action {transmit | drop} |
exceed-action {transmit | drop | policed-dscp-transmit}]
```

```
no qos aggregate-policer name
```

Syntax Description

<i>name</i>	Name of the aggregate policer.
<i>rate</i>	Maximum bits per second; valid values are from 32000 to 32000000000.
<i>burst</i>	Burst bytes; valid values are from 1000 to 512000000.
conform-action	(Optional) Specifies the action to be taken when the rate is not exceeded.
transmit	(Optional) Transmits the package.
drop	(Optional) Drops the packet.
exceed-action	(Optional) Specifies action when QoS values are exceeded.
policed-dscp-transmit	(Optional) Sends the DSCP per the policed-DSCP map.

Defaults

The default settings are as follows:

- Conform-action transmits
- Exceed-action drops

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

This policer can be shared by different policy map classes and on different interfaces.

The Catalyst 4006 switch supports up to 1000 aggregate input policers and 1000 output policers.

The **qos aggregate-policer** command allows you to configure an aggregate flow and a policing rule for that aggregate. When you enter your rate and burst parameters, the range for the average rate is 32 Kbps to 32 Gbps, and the range for the burst size is 1 KB to 512 MB.

A rate can be entered in bits-per-second without a suffix. In addition, the suffixes described in [Table 2-10](#) are allowed.

Table2-10 Rate Suffix

Suffix	Description
k	1000 bps
m	1,000,000 bps
g	1,000,000,000 bps

Bursts can be entered in bytes without a suffix. In addition, the suffixes shown in [Table2-11](#) are allowed.

Table2-11 Burst Suffix

Suffix	Description
k	1000 bytes
m	1,000,000 bytes
g	1,000,000,000 bytes

**Note**

Due to hardware granularity, the rate value is limited, so the burst you configure might not be the value that is used.

Modifying an existing aggregate rate limit modifies that entry in NVRAM as well as in the switch if it is currently being used.

When you enter the aggregate policer name, follow these naming conventions:

- Maximum of 31 characters long and may include a-z, A-Z, 0-9, the dash (-), the underscore (_), and the period (.).
- Must start with an alphabetic character and must be unique across all ACLs of all types.
- Aggregate policer names are case sensitive.
- Cannot be a number.
- Must not be a keyword; keywords to avoid are **all**, **default-action**, **map**, **help**, and **editbuffer**.

An aggregate policer can be applied to one or more interfaces. However, if you apply the same policer to the input direction on one interface and to the output direction on a different interface, then you have created the equivalent of two different aggregate policers in the switching engine. Each policer has the same policing parameters, with one policing the ingress traffic on one interface and the other policing the egress traffic on another interface. If you apply an aggregate policer to multiple interfaces in the same direction, only one instance of the policer is created in the switching engine.

Similarly, you can apply an aggregate policer to a physical interface or to a VLAN. If you apply the same aggregate policer to a physical interface and to a VLAN, then you have created the equivalent of two different aggregate policers in the switching engine. Each policer has the same policing parameters, with one policing the traffic on the configured physical interface and the other policing the traffic on the configured VLAN. If you apply an aggregate policer to only ports or only VLANs, then only one instance of the policer is created in the switching engine.

In effect, if you apply a single aggregate policer to ports and VLANs in different directions, then you have created the equivalent of four aggregate policers; one for all ports sharing the policer in input direction, one for all ports sharing the policer in output direction, one for all VLANs sharing the policer in input direction, and one for all VLANs sharing the policer in output direction.

■ qos aggregate-policer

Examples

This example shows how to configure a QoS aggregate policer to allow a maximum of 100,000 bits per second with a normal burst size of 10,000 bytes, to transmit when these rates are not exceeded, and to drop packets when these rates are exceeded:

```
Switch(config)# qos aggregate-policer micro-one 100000 10000 conform-action transmit exceed action drop
Switch(config)#
```

Related Commands

[show qos aggregate policer](#)

qos cos

To define the default CoS value for an interface, use the **qos cos** command. To remove a prior entry, use the **no** form of this command.

qos cos *cos_value*

no qos cos *cos_value*

Syntax Description	<i>cos_value</i> Default CoS value for the interface; valid values are from 0 to 7.
---------------------------	---

Defaults	The default CoS value is 0.
-----------------	-----------------------------



Note	CoS override is not configured.
-------------	---------------------------------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	CoS values are configurable on physical LAN ports only.
-------------------------	---

Examples	This example shows how to configure the default QoS CoS value as 6:
-----------------	---

```
Switch(config-if)# qos cos 6
Switch(config-if)#
```

Related Commands	show qos
-------------------------	--------------------------

qos dbl

To enable Dynamic Buffer Limiting (DBL) globally on the switch, use the **qos dbl** command. To disable DBL, use the **no** form of this command.

```
qos dbl [buffers {aggressive-flow buffers} | credits {aggressive-flow credits |
maximum max} | exceed-action {ecn | probability percent} |
flow {include [layer4-ports] [vlan]}}
```

```
no qos dbl [buffers {aggressive-flow buffers} | credits {aggressive-flow credits |
maximum max} | exceed-action {ecn | probability percent} |
flow {include [layer4-ports] [vlan]}}
```

Syntax Description

buffers	(Optional) Specifies buffer limit for aggressive flows.
aggressive-flow	(Optional) Specifies aggressive flow.
<i>buffers</i>	(Optional) Number of buffers for aggressive flows; valid values are from 0 to 255.
credits	(Optional) Specifies credit limit for aggressive flows and all flows.
<i>credits</i>	(Optional) Number of credits for aggressive flows; valid values are from 0 to 15.
maximum	(Optional) Specifies maximum credit for all flows.
<i>max</i>	(Optional) Number of credits for all flows; valid values are from 0 to 15.
exceed-action	(Optional) Specifies packet marking when limits are exceeded.
ecn	(Optional) Specifies explicit congestion notification.
probability	(Optional) Specifies probability of packet marking.
<i>percent</i>	(Optional) Probability number; valid values are from 0 to 100.
flow	(Optional) Specifies flows for limiting.
include	(Optional) Allows Layer 4 ports and VLANs to be included in flows.
layer4-ports	(Optional) Includes Layer 4 ports in flows.
vlan	(Optional) Includes VLANs in flows.

Defaults

The default settings are as follows:

- QoS DBL is disabled.
- Aggressive-flow buffers is set to 2.
- Aggressive-flow credits is set to 2.
- Layer 4 ports are included.
- VLANs are included.
- 15 maximum credits are allowed.
- 15% drop probability is set.

Command Modes

Global configuration

QoS policy-map class configuration

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

This example shows how to enable DBL globally on the switch:

```
Switch(config)# qos db1
Global DBL enabled
Switch(config)#
```

This example shows how to enable DBL in the QoS policy-map class configuration mode:

```
Switch(config)# class-map c1
Switch(config-cmap)# policy p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# db1
Switch(config-pmap-c)#
```

Related Commands

[show qos db1](#)

qos dscp

To define the default CoS value for an interface, use the **qos dscp** command. To remove a prior entry, use the **no** form of this command.

```
qos dscp dscp_value
```

```
no qos dscp dscp_value
```

Syntax Description	<i>dscp_value</i> Default DSCP value for the interface; valid values are from 0 to 63.
---------------------------	--

Defaults	The default DSCP value is 0.
-----------------	------------------------------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples	This example shows how to configure the default QoS DSCP value as 6:
-----------------	--

```
Switch(config-if)# qos dscp 6
Switch(config-if)#
```

Related Commands	show qos interface
-------------------------	------------------------------------

qos map cos

To define the ingress CoS-to-DSCP mapping for trusted interfaces, use the **qos map cos** command. To remove a prior entry, use the **no** form of this command.

```
qos map cos cos_values to dscp dscp1
```

```
no qos map cos to dscp
```

Syntax Description

<i>cos_values</i>	CoS values, list up to eight CoS values separated by spaces.
to dscp	Defines mapping and specifies DSCP value.
<i>dscp1</i>	DSCP value to map to the CoS values; valid values are from 0 to 63.

Defaults

The default CoS-to-DSCP configuration settings are shown in the following table:

CoS	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The CoS-to-DSCP map is used to map the packet CoS (on interfaces configured to trust CoS) to the internal DSCP value. This map is a table of eight CoS values (0 through 7) and their corresponding DSCP value. The switch has one map.

Examples

This example shows how to configure the ingress CoS-to-DSCP mapping for cos 0:

```
Switch(config)# qos map cos 0 to dscp 20
Switch(config)#
```

This example shows how to disable the ingress CoS-to-DSCP mapping for cos 0:

```
Switch(config)# no qos map cos 0 to dscp 20
Switch(config)#
```

Related Commands

[qos map dscp](#)
[qos map dscp policed](#)
[show qos](#)

qos map dscp

To map DSCP values to selected transmit queues and to map the DSCP-to-CoS value, use the **qos map dscp** command. To return to the default value, use the **no** form of this command.

qos map dscp *dscp-values* **to tx-queue** *queue-id*

no qos map dscp *dscp-values* **to cos** *cos-value*

Syntax Description

<i>dscp-values</i>	List of DSCP values to map to the queue ID; valid values are from 0 to 63.
to	Defines mapping.
tx-queue	Specifies a transmit queue.
<i>queue-id</i>	Transmit queue; valid values are from 1 to 4.
cos	Specifies the CoS value.
<i>cos-value</i>	Class of service; valid values are from 1 to 7.

Defaults

The default DSCP-to-CoS configuration settings are shown in the following table:

DSCP	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
CoS	0	1	2	3	4	5	6	7

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

You use the DSCP-to-CoS map to map the final DSCP classification to a final CoS. The CoS map is written into the ISL header or 802.1Q tag of the transmitted packet on trunk interfaces and contains a table of 64 DSCP values and the corresponding CoS values. The switch has one map. You can enter up to eight DSCP values, separated by spaces, for a CoS value.

The DSCP-to-transmit-queue map is used to map the final DSCP classification to a transmit queue. You can enter up to eight DSCP values, separated by spaces, for a transmit queue.

Examples

This example shows how to configure the egress DSCP-to-CoS mapping:

```
Switch(config)# qos map dscp 20 25 to cos 3
Switch(config)#
```

This example shows how to configure the egress DSCP-to-transmit queue:

```
Switch(config)# qos map dscp 20 25 to tx-queue 1
Switch(config)#
```

Related Commands

qos map cos
show qos interface
show qos
tx-queue

qos map dscp policed

To set the mapping of policed DSCP values to marked-down DSCP values, use the **qos map dscp policed** command. To remove a prior entry, use the **no** form of this command.

```
qos map dscp policed dscp_list to dscp policed_dscp
```

```
no qos map dscp policed
```

Syntax Description

<i>dscp_list</i>	DSCP values; valid values are from 0 to 63.
to dscp	Defines mapping.
<i>policed_dscp</i>	Marked-down DSCP values; valid values are from 0 to 63.

Defaults

Mapping of DSCP values is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The DSCP-to-policed-DSCP map determines the marked-down DSCP value applied to out-of-profile flows. The switch has one map.

You can enter up to eight DSCP values, separated by spaces.

You can enter only one policed DSCP value.



Note

To avoid out-of-sequence packets, configure the DSCP-to-policed-DSCP map so that marked-down packets remain in the same queue as in-profile traffic.

Examples

This example shows how to map multiple DSCPs to a single policed-DSCP value:

```
Switch(config)# qos map dscp policed 20 25 43 to dscp 4
Switch(config)#
```

Related Commands

[qos map cos](#)
[qos map dscp](#)
[show qos](#)

qos rewrite ip dscp

To enable DSCP rewrite for IP packets, use the **qos rewrite ip dscp** command. To disable IP DSCP rewrite, use the **no** form of the command.

qos rewrite ip dscp

no qos rewrite ip dscp

Syntax Description This command has no arguments or keywords.

Defaults IP DSCP rewrite is enabled.

Command Modes Global configuration

Command History	Release	Modification
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines If you disable IP DSCP rewrite and enable QoS globally, the following events occur:

- The ToS byte on the IP packet is not modified.
- Marked and marked-down DSCP values are used for queueing.
- The internally derived DSCP (as per the trust configuration on the interface or VLAN policy) is used for transmit queue and Layer 2 CoS determination. The DSCP is not rewritten on the IP packet header.

If you disable QoS, the CoS and DSCP of the incoming packet are preserved and are not rewritten.

Examples The following example shows how to disable IP DSCP rewrite:

```
Switch(config)# no qos rewrite ip dscp
Switch(config)#
```

Related Commands **qos (global configuration mode)**
[show qos](#)

qos trust

To set the trusted state of an interface (for example, whether the packets arriving at an interface are trusted to carry the correct CoS, TOS, and DSCP classifications), use the **qos trust** command. To set an interface to the untrusted state, use the **no** form of this command.

```
qos trust {cos | device cisco-phone | dscp | extend [cos priority]}
```

```
no qos trust {cos | device cisco-phone | dscp | extend [cos priority]}
```

Syntax Description

cos	Specifies that the CoS bits in incoming frames are trusted and derives the internal DSCP value from the CoS bits.
<i>device cisco-phone</i>	Specifies the Cisco IP phone as the trust device for a port.
dscp	Specifies that the TOS bits in the incoming packets contain a DSCP value.
extend	Specifies extending trust to Port VLAN ID (PVID) packets coming from the PC.
<i>cos priority</i>	(Optional) CoS priority value set to PVID packets; valid values are from 0 to 7.

Defaults

The default settings are as follows:

- If global QoS is enabled, trust is disabled on the port.
- If global QoS is disabled, trust DSCP is enabled on the port.
- The CoS priority level is 0.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(11)EW	Support for extending trust for voice was added.
12.1(19)EW	Support for trust device Cisco IP phone.

Usage Guidelines

You can only configure the trusted state on physical LAN interfaces.

By default, the trust state of an interface when QoS is enabled is untrusted; when QoS is disabled on the interface, the trust state is reset to trust DSCP.

When the interface trust state is **qos trust cos**, the transmit CoS is always the incoming packet CoS (or the default CoS for the interface, if the packet is not tagged).

When the interface trust state is not **qos trust dscp**, security and QoS ACL classification will always use the interface DSCP and not the incoming packet DSCP.

Trusted Boundary should not be configured on ports that are part of an EtherChannel (that is, port channel).

Examples

This example shows how to set the trusted state of an interface to CoS:

```
Switch(config-if)# qos trust cos
Switch(config-if)#
```

This example shows how to set the trusted state of an interface to DSCP:

```
Switch(config-if)# qos trust dscp
Switch(config-if)#
```

This example shows how to set the PVID CoS level to 6:

```
Switch(config-if)# qos trust extend cos 6
Switch(config-if)#
```

This example shows how to set the Cisco phone as the trust device:

```
Switch(config-if)# qos trust device cisco-phone
Switch(config-if)#
```

Related Commands

[qos cos](#)
[qos vlan-based](#)
[show qos interface](#)

qos vlan-based

To enable per-VLAN QoS for a Layer 2 interface, use the **qos vlan-based** command. To disable per-VLAN QoS for a Layer 2 interface, use the **no** form of this command.

qos vlan-based

no qos vlan-based

Syntax Description This command has no arguments or keywords.

Defaults Per-VLAN QoS is disabled.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

In VLAN-based mode, the policy map attached to the Layer 2 interface is ignored, and QoS is driven by the policy map attached to the corresponding VLAN interface.

Per-VLAN QoS can be configured only on Layer 2 interfaces.

If no input QoS policy is attached to a Layer 2 interface, then the input QoS policy attached to the VLAN (on which the packet is received), if any, is used even if the port is not configured as VLAN-based.

If you do not want this default, attach a placeholder input QoS policy to the Layer 2 interface.

Similarly, if no output QoS policy is attached to a Layer 2 interface, then the output QoS policy attached to the VLAN (on which the packet is transmitted), if any, is used even if the port is not configured as VLAN-based.

If you do not want this default, attach a placeholder output QoS policy to the Layer 2 interface.

Layer 3 interfaces are always in interface-based mode. Layer 3 VLAN interfaces are always in VLAN-based

Examples This example shows how to enable per-VLAN QoS for a Layer 2 interface:

```
Switch(config-if)# qos vlan-based
Switch(config-if)#
```

Related Commands

- [qos cos](#)
- [show qos interface](#)

redundancy

To enter the redundancy configuration mode, use the **redundancy** command in the global configuration mode.

redundancy

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Global configuration

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch. (Catalyst 4507R only)

Usage Guidelines

The redundancy configuration mode is used to enter the main CPU submode.

To enter the main CPU submode, use the **main-cpu** command in the redundancy configuration mode. The main CPU submode is used to manually synchronize the configurations on the two supervisor engines.

From the main CPU submode, use the **auto-sync** command to enable automatic synchronization of the configuration files in NVRAM.

Use the **no** command to disable redundancy. If you disable redundancy, then reenabling redundancy, the switch returns to default redundancy settings.

Use the **exit** command to exit the redundancy configuration mode.

Examples This example shows how to enter redundancy mode:

```
Switch(config)# redundancy
Switch(config-r)#
```

This example shows how to enter the main CPU submode:

```
Switch(config)# redundancy
Switch(config-red)# main-cpu
Switch(config-r-mc)#
```

Related Commands [auto-sync](#)
[main-cpu](#)

redundancy force-switchover

To force a switchover from the active to the standby supervisor engine, use the **redundancy force-switchover** command.

redundancy force-switchover

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes EXEC

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch (Catalyst 4507R only.)

Usage Guidelines Before using this command, refer to the “Performing a Software Upgrade” section of the *Catalyst4500 Series Switch CiscoIOS Software Configuration Guide* for additional information.

The **redundancy force-switchover** command conducts a manual switchover to the redundant supervisor engine. The redundant supervisor engine becomes the new active supervisor engine running the CiscoIOS image. The modules are reset.

The old active supervisor engine reboots with the new image and becomes the standby supervisor engine.

Examples This example shows how to switch over manually from the active to the standby supervisor engine:

```
Switch# redundancy force-switchover
Switch#
```

Related Commands [redundancy](#)
[show redundancy](#)

redundancy reload

To force a reload of one or both supervisor engines, use the **redundancy reload** command.

redundancy reload { peer | shelf }

Syntax Description	peer	Reloads the peer unit.
	shelf	Reboots both supervisor engines.

Defaults This command has no default settings.

Command Modes EXEC

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch (Catalyst 4507R only.)

Usage Guidelines Before using this command, refer to the “Performing a Software Upgrade” section of the *Catalyst4500 Series Switch Cisco IOS Software Configuration Guide* for additional information.

The **redundancy reload shelf** command conducts a reboot of both supervisor engines. The modules are reset.

Examples This example shows how to manually reload one or both supervisor engines:

```
Switch# redundancy reload shelf
Switch#
```

Related Commands [redundancy](#)
[show redundancy](#)

remote login module

To remotely connect to a specific module, use the **remote login module** configuration command.

remote login module *mod*

Syntax Description	<i>mod</i> Target module for the command.
---------------------------	---

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.1(19)EW	This command was first introduced.

Usage Guidelines	<p>This command applies only to the Access Gateway Module on Catalyst 4500 series switches.</p> <p>The valid values for <i>mod</i> depends on the chassis used. For example, if you have a Catalyst 4006 chassis, valid values for the module are from 2 to 6. If you have a 4507R chassis, valid values are from 3 to 7.</p> <p>When you execute the remote login module <i>mod</i> command, the prompt changes to Gateway#</p> <p>The remote login module command is identical to the session module <i>mod</i> and the attach module <i>mod</i> commands.</p>
-------------------------	--

Examples	This example shows how to remotely log in to the Access Gateway Module:
-----------------	---

```
Switch# remote login module 5
Attaching console to module 5
Type 'exit' at the remote prompt to end the session

Gateway>
```

Related Commands	attach module session module
-------------------------	---

remote-span

To convert a VLAN into an RSPAN VLAN, use the **remote-span** command. To convert an RSPAN VLAN to a VLAN, use the **no** form of this command.

remote-span

no remote-span

Syntax Description This command has no arguments or keywords.

Defaults RSPAN is disabled.

Command Modes VLAN configuration

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to convert a VLAN into an RSPAN VLAN:

```
Switch# config terminal
Switch(config)# vlan 20
Switch(config-vlan)# remote-span
Switch(config-vlan)# end
Switch#
```

Related Commands [monitor session](#)

renew ip dhcp snooping database

To renew the DHCP binding database, use the **renew ip dhcp snooping database** command.

renew ip dhcp snooping database [validation none] [url]

Syntax Description	validation none	(Optional) Specifies that the checksum associated with the contents of the file specified by the URL is not verified.
	url	(Optional) Specifies the file from which the read is performed.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines If the URL is not provided, the switch tries to read the file from the configured URL.

Examples This example shows how to renew the DHCP binding database, while bypassing the CRC checks:

```
Switch# renew ip dhcp snooping database validation none
Switch#
```

Related Commands

- [ip dhcp snooping](#)
- [ip dhcp snooping binding](#)
- [ip dhcp snooping information option](#)
- [ip dhcp snooping trust](#)
- [ip dhcp snooping vlan](#)
- [show ip dhcp snooping](#)
- [show ip dhcp snooping binding](#)

reset

To leave the proposed new VLAN database but remain in VLAN configuration mode and reset the proposed new database to be identical to the VLAN database currently implemented, use the **reset** command.

reset

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes VLAN configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples In this example, the proposed new VLAN database is reset to the current VLAN database:

```
Switch(vlan-config)# reset
RESET completed.
Switch(vlan-config)#
```

revision

To set the MST configuration revision number, use the **revision** command. To return to the default settings, use the **no** form of this command.

revision *version*

no revision

Syntax Description	<i>version</i> Configuration revision number; valid values are from 0 to 65535.
---------------------------	---

Defaults	Revision version is set to 0.
-----------------	-------------------------------

Command Modes	MST configuration
----------------------	-------------------

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	If two Catalyst 4500 series switches have the same configuration but have different configuration revision numbers, they are considered to be part of two different regions.
-------------------------	--



Caution

Be careful when using the **revision** command to set the MST configuration revision number because a mistake can put the switch in a different region.

Examples	This example shows how to set the configuration revision number:
-----------------	--

```
Switch(config-mst)# revision 5
Switch(config-mst)#
```

Related Commands	<p>instance</p> <p>name</p> <p>show spanning-tree mst</p> <p>spanning-tree mst configuration</p>
-------------------------	--

service-policy

To attach a policy map to an interface, use the **service-policy** command. To remove a policy map from an interface, use the **no** form of this command.

service-policy { **input** | **output** } *policy-map name*

no service-policy { **input** | **output** } *policy-map name*

Syntax Description	input	Specifies input policy maps.
	output	Specifies output policy maps.
	<i>policy-map name</i>	Name of a previously configured policy map.

Defaults A policy map is not attached to an interface.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to attach a policy map to a Fast Ethernet interface:

```
Switch(config)# interface fastethernet 5/20
Switch(config-if)# service-policy input pmap1
Switch(config-if)#
```

Related Commands [class-map](#)
[policy-map](#)

session module

To remotely connect to a specific module, use the **session module** configuration command.

session module *mod*

Syntax Description	<i>mod</i>	Target module for the command.
---------------------------	------------	--------------------------------

Defaults	This command has no default settings.	
-----------------	---------------------------------------	--

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

Command History	Release	Modification
	12.1(19)EW	This command was first introduced.

Usage Guidelines	<p>This command applies only to the Access Gateway Module on Catalyst 4500 series switches.</p> <p>The valid values for <i>mod</i> depends on the chassis used. For example, if you have a Catalyst 4006 chassis, valid values for the module are from 2 to 6. If you have a 4507R chassis, valid values are from 3 to 7.</p> <p>When you execute the session module <i>mod</i> command, the prompt changes to Gateway#.</p> <p>The session command is identical to the attach module <i>mod</i> and the remote login module <i>mod</i> commands.</p>
-------------------------	--

Examples	This example shows how to remotely log in to the Access Gateway Module:
-----------------	---

```
Switch# session module 5
Attaching console to module 5
Type 'exit' at the remote prompt to end the session

Gateway>
```

Related Commands	<p>attach module</p> <p>remote login module</p>
-------------------------	---

shape

To specify traffic shaping on an interface, use the **shape** command. Use the **no** form of this command to remove traffic shaping.

shape [rate] [percent]

no shape [rate] [percent]

Syntax Description	rate	(Optional) Specifies an average rate for traffic shaping. The range is 16000 to 1000000000. Postfix notation (k, m, and g) is optional and a decimal point is allowed.
	percent	(Optional) Specifies a percent of bandwidth for traffic shaping.

Defaults Default is no traffic shaping.

Command Modes Interface transmit queue configuration mode

Command History	Release	Modification
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Traffic shaping is available on all the port, and it sets an upper limit on the bandwidth. When high shape rates are configured on the Catalyst 4500 Supervisor Engine V (WS-X4516), the shaped traffic rate may not be achieved in situations that involve contention and unusual packet size distributions. On ports that are multiplexed through a Stub ASIC and connected to the backplane gigaports, shape rates above 7 megabits per second may not be achieved under worst-case conditions. On ports that are connected directly to the backplane gigaports, or the supervisor engine gigaports, shape rates above 50 megabits per second may not be achieved under worst-case conditions.

Some examples of ports connected directly to the backplane are as follows:

- Uplink ports on Supervisor Engine II+, III, IV, and V
- Ports on the WS-X4306-GB module
- The two 1000BASE-X ports on the WS-X4232-GB-RJ module
- The first two ports on the WS-X4418-GB module
- The two 1000BASE-X ports on the WS-X4412-2GB-TX module

All ports on 24-port modules and 48-port modules are multiplexed through a Stub ASIC. Some examples of ports multiplexed through a Stub ASIC are:

- 10/100 ports on the WS-X4148-RJ45 module
- 10/100/1000 ports on the WS-X4124-GB-RJ45 module
- 10/100/1000 ports on the WS-X4448-GB-RJ45 module

Examples

The following example shows how to configure a maximum bandwidth (70 percent) for the interface fa3/1:

```
Switch(config)# interface fastethernet3/1
Switch(config-if)# tx-queue 3
Switch(config-if-tx-queue)# shape 70m
Switch(config-if-tx-queue)#
```

show access-group mode interface

To display the ACL configuration on a Layer 2 interface, use the **show mac access-group interface** command.

show access-group mode interface [*interface interface-number*]

Syntax Description	<i>interface</i>	(Optional) Interface type; valid values are ethernet , FastEthernet , GigabitEthernet , and port-channel .
	<i>interface-number</i>	(Optional) Interface number.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
		12.1(19)EW

Usage Guidelines Valid values for the port number depend on the chassis used.

Examples This example shows how to display the ACL configuration on interface fast 6/1:

```
Switch# show access-group mode interface fast 6/1
Interface FastEthernet6/1:
  Access group mode is: merge
```

Related Commands [access-group mode](#)

show arp access-list

To display detailed information on an ARP access list, use the **show arp** command.

show arp access-list

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes EXEC

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to display the ARP ACL information for a switch:

```
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

- [access-group mode](#)
- [arp access-list](#)
- [ip arp inspection filter vlan](#)

show auto qos

To display the automatic quality of service (auto-QoS) configuration that is applied, use the **show auto qos** user EXEC command.

```
show auto qos [interface interface-id] [{begin | exclude | include} expression]
```

Syntax Description	Parameter	Description
	interface <i>interface-id</i>	(Optional) Displays auto-QoS information for the specified interface or for all interfaces. Valid interfaces include physical ports.
	begin	(Optional) Begins with the line that matches the expression.
	exclude	(Optional) Excludes lines that match the expression.
	include	(Optional) Includes lines that match the specified expression.
	<i>expression</i>	(Optional) Expression in the output to use as a reference point.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines The **show auto qos interface** *interface-id* command displays the auto-QoS configuration; it does not display any user changes to the configuration that might be in effect.

To display information about the QoS configuration that might be affected by auto-QoS, use one of these commands:

- **show qos**
- **show qos map**
- **show qos interface** *interface-id*
- **show running-config**

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 output from the **show auto qos** command when auto-QoS is enabled:

```
Switch# show auto qos
00:00:55:qos
00:00:56:qos map cos 3 to dscp 26
00:00:57:qos map cos 5 to dscp 46
00:00:58:qos map dscp 16 to tx-queue 1
00:00:58:qos map dscp 32 to tx-queue 1
00:00:58:qos db1
00:00:59:policy-map autoqos-voip-policy
00:00:59:  class class-default
00:00:59:    db1
00:00:59:interface GigabitEthernet1/1
00:00:59:  qos trust device cisco-phone
00:00:59:  qos trust cos
00:00:59:  tx-queue 3
00:00:59:  priority high
00:00:59:  shape percent 70
00:00:59:  service-policy output autoqos-voip-policyend
```

This example shows output from the **show auto qos interface** command when the **auto qos voip cisco-phone** interface configuration command is entered:

```
Switch# show auto qos interface
Initial configuration applied by AutoQoS:
!
interface GigabitEthernet1/1
qos trust device cisco-phone
qos trust cos
tx-queue 3
priority high
shape percent 70
service-policy output autoqos-voip-policy
!
interface GigabitEthernet1/2
qos trust device cisco-phone
qos trust cos
tx-queue 3
priority high
shape percent 70
service-policy output autoqos-voip-policy
```

This example shows output from the **show auto qos interface gigabitethernet1/1** command when the **auto qos voip cisco-phone** interface configuration command is entered:

```
Switch# show auto qos interface gigabitethernet1/1
Initial configuration applied by AutoQoS:
!
interface GigabitEthernet1/1
qos trust device cisco-phone
qos trust cos
tx-queue 3
priority high
shape percent 70
service-policy output autoqos-voip-policy
```

This example shows output from the **show auto qos** command when auto-QoS is disabled:

```
Switch# show auto qos
AutoQoS is disabled
```

Related Commands

auto qos voip

show bootflash:

To display information about the bootflash: file system, use the **show bootflash:** command.

show bootflash: [**all** | **chips** | **fileSYS**]

Syntax Description	all	(Optional) Displays all possible Flash information.
	chips	(Optional) Displays Flash chip information.
	fileSYS	(Optional) Displays file system information.

Defaults This command has no default settings.

Command Modes EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to display file system status information:

```
Switch> show bootflash: fileSYS

----- F I L E   S Y S T E M   S T A T U S -----
  Device Number = 0
DEVICE INFO BLOCK: bootflash
  Magic Number      = 6887635   File System Vers = 10000   (1.0)
  Length            = 1000000   Sector Size      = 40000
  Programming Algorithm = 39     Erased State     = FFFFFFFF
  File System Offset = 40000     Length           = F40000
  MONLIB Offset     = 100        Length           = C628
  Bad Sector Map Offset = 3FFF8   Length           = 8
  Squeeze Log Offset = F80000    Length           = 40000
  Squeeze Buffer Offset = FC0000   Length           = 40000
  Num Spare Sectors = 0
    Spares:
STATUS INFO:
  Writable
  NO File Open for Write
  Complete Stats
  No Unrecovered Errors
  No Squeeze in progress
USAGE INFO:
  Bytes Used      = 917CE8   Bytes Available = 628318
  Bad Sectors    = 0        Spared Sectors  = 0
  OK Files       = 2         Bytes           = 917BE8
  Deleted Files  = 0         Bytes           = 0
  Files w/Errors = 0         Bytes           = 0
Switch>
```

show bootflash:

This example shows how to display system image information:

```
Switch> show bootflash:
-# - ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
1  .. image      8C5A393A  237E3C   14  2063804 Aug 23 1999 16:18:45 c4-boot-mz
2  .. image      D86EE0AD  957CE8    9   7470636 Sep 20 1999 13:48:49 rp.halley
Switch>
```

This example shows how to display all bootflash information:

```
Switch> show bootflash: all
-# - ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
1  .. image      8C5A393A  237E3C   14  2063804 Aug 23 1999 16:18:45 c4-boot-
mz
2  .. image      D86EE0AD  957CE8    9   7470636 Sep 20 1999 13:48:49 rp.halley

6456088 bytes available (9534696 bytes used)

----- F I L E   S Y S T E M   S T A T U S -----
Device Number = 0
DEVICE INFO BLOCK: bootflash
  Magic Number      = 6887635   File System Vers = 10000   (1.0)
  Length            = 1000000   Sector Size      = 40000
  Programming Algorithm = 39     Erased State     = FFFFFFFF
  File System Offset = 40000    Length = F40000
  MONLIB Offset     = 100      Length = C628
  Bad Sector Map Offset = 3FFF8   Length = 8
  Squeeze Log Offset = F80000   Length = 40000
  Squeeze Buffer Offset = FC0000   Length = 40000
  Num Spare Sectors = 0
  Spares:
STATUS INFO:
  Writable
  NO File Open for Write
  Complete Stats
  No Unrecovered Errors
  No Squeeze in progress
USAGE INFO:
  Bytes Used      = 917CE8   Bytes Available = 628318
  Bad Sectors    = 0        Spared Sectors = 0
  OK Files       = 2        Bytes = 917BE8
  Deleted Files  = 0        Bytes = 0
  Files w/Errors = 0        Bytes = 0
Switch>
```

show bootvar

To display BOOT environment variable information, use the **show bootvar** command.

show bootvar

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to display BOOT environment variable information:

```
Switch# show bootvar
BOOT variable = sup:1;
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x0
Switch#
```

show class-map

To display class map information, use the **show class-map** command.

show class-map *class_name*

Syntax Description	<i>class_name</i> Name of the class map.				
Defaults	This command has no default settings.				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(8a)EW</td> <td>Support for this command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Release	Modification				
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.				

Examples

This example shows how to display class map information for all class maps:

```
Switch# show class-map
Class Map match-any class-default (id 0)
  Match any
Class Map match-any class-simple (id 2)
  Match any
Class Map match-all ipp5 (id 1)
  Match ip precedence 5
Class Map match-all agg-2 (id 3)
Switch#
```

This example shows how to display class map information for a specific class map:

```
Switch# show class-map ipp5
Class Map match-all ipp5 (id 1)
  Match ip precedence 5
Switch#
```

Related Commands

[class-map](#)
[show policy-map](#)
[show policy-map interface](#)

show diagnostic result module

To display module-based diagnostic test results, use the **show diagnostic result module** command.

show diagnostic result module [*slot-num* / **all**] [**test** [*test-id* / *test-id-range* / **all**]] [**detail**]

Syntax Description	
<i>slot-num</i>	(Optional) Specifies the slot on which diagnostics are displayed.
all	(Optional) Displays diagnostics for all slots.
test	(Optional) Displays selected tests on the specified module.
<i>test-id</i>	(Optional) Specifies a single test ID.
<i>test-id-range</i>	(Optional) Specifies a range of test IDs.
all	(Optional) Displays diagnostics for all tests.
detail	(Optional) Displays complete test results.

Defaults A summary of the test results for all modules in the chassis is displayed.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to display the summary results for all modules in the chassis:

```
Switch# show diagnostic result module

Current bootup diagnostic level: minimal

module 1:

  Overall diagnostic result: PASS
  Diagnostic level at card bootup: bypass

  Test results: (. = Pass, F = Fail, U = Untested)

    1) supervisor-bootup -----> U
    2) packet-memory-bootup -----> U
    3) packet-memory-ongoing -----> U

module 4:

  Overall diagnostic result: PASS
  Diagnostic level at card bootup: minimal

  Test results: (. = Pass, F = Fail, U = Untested)

    1) linecard-online-diag -----> .
```

```

module 5:

Overall diagnostic result: PASS
Diagnostic level at card bootup: minimal

Test results: (. = Pass, F = Fail, U = Untested)

1) linecard-online-diag -----> .

```

```

module 6:

Overall diagnostic result: PASS
Diagnostic level at card bootup: minimal

Test results: (. = Pass, F = Fail, U = Untested)

1) linecard-online-diag -----> .

```

This example shows how to display online diagnostics for module 1:

```

Switch# show diagnostic result module 1 detail

Current bootup diagnostic level: minimal

module 1:

Overall diagnostic result: PASS
Diagnostic level at card bootup: minimal

Test results: (. = Pass, F = Fail, U = Untested)

-----

1) supervisor-bootup -----> .

Error code -----> 0 (DIAG_SUCCESS)
Total run count -----> 0
Last test execution time -----> n/a
First test failure time -----> n/a
Last test failure time -----> n/a
Last test pass time -----> n/a
Total failure count -----> 0
Consecutive failure count -----> 0

Power-On-Self-Test Results for ACTIVE Supervisor

Power-on-self-test for Module 1: WS-X4014
Port/Test Status: (. = Pass, F = Fail)
Reset Reason: PowerUp Software/User

Port Traffic: L2 Serdes Loopback ...
0: . 1: . 2: . 3: . 4: . 5: . 6: . 7: . 8: . 9: . 10: . 11: .
12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .
24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: .

```



```
Port Traffic: L2 Asic Loopback ...
0: . 1: . 2: . 3: . 4: . 5: . 6: . 7: . 8: . 9: . 10: . 11: .
12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .
24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: .
```

```
Port Traffic: L3 Asic Loopback ...
0: . 1: . 2: . 3: . 4: . 5: . 6: . 7: . 8: . 9: . 10: . 11: .
12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .
24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: . au: .
```

```
Switch Subsystem Memory ...
1: . 2: . 3: . 4: . 5: . 6: . 7: . 8: . 9: . 10: . 11: . 12: .
13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: . 24: .
25: . 26: . 27: . 28: . 29: . 30: . 31: . 32: . 33: . 34: . 35: . 36: .
37: . 38: . 39: . 40: . 41: . 42: . 43: . 44: . 45: . 46: . 47: . 48: .
49: . 50: . 51: . 52: . 53: . 54: .
```

Module 1 Passed

```
2) packet-memory-bootup -----> .

    Error code -----> 0 (DIAG_SUCCESS)
    Total run count -----> 0
    Last test execution time -----> n/a
    First test failure time -----> n/a
    Last test failure time -----> n/a
    Last test pass time -----> n/a
    Total failure count -----> 0
    Consecutive failure count -----> 0
packet buffers on free list: 64557 bad: 0 used for ongoing tests: 979
```

```
Number of errors found: 0
Cells with hard errors (failed two or more tests): 0
Cells with soft errors (failed one test, includes hard): 0
Suspect bad cells (uses a block that tested bad): 0
total buffers: 65536
bad buffers: 0 (0.0%)
good buffers: 65536 (100.0%)
Bootup test results:1
No errors.
```

```
3) packet-memory-ongoing -----> U

    Error code -----> 0 (DIAG_SUCCESS)
    Total run count -----> 0
    Last test execution time -----> n/a
    First test failure time -----> n/a
    Last test failure time -----> n/a
    Last test pass time -----> n/a
    Total failure count -----> 0
    Consecutive failure count -----> 0
packet buffers on free list: 64557 bad: 0 used for ongoing tests: 979
```

show diagnostic result module

```

Packet memory errors: 0 0
Current alert level: green
Per 5 seconds in the last minute:
  0 0 0 0 0 0 0 0 0 0
  0 0
Per minute in the last hour:
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
Per hour in the last day:
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0
Per day in the last 30 days:
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
Direct memory test failures per minute in the last hour:
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
Potential false positives: 0 0
Ignored because of rx errors: 0 0
Ignored because of cdm fifo overrun: 0 0
Ignored because of oir: 0 0
Ignored because isl frames received: 0 0
Ignored during boot: 0 0
Ignored after writing hw stats: 0 0
Ignored on high gigaport: 0
Ongoing diag action mode: Normal
Last 1000 Memory Test Failures:
Last 1000 Packet Memory errors:
First 1000 Packet Memory errors:

```

Switch#

show diagnostic result module test 2

To display the results of the bootup packet memory test, use the **show diagnostic result module test 2** command. The output indicates whether the test passed, failed, or was not run.

show diagnostic result module *N* test 2 [detail]

Syntax Description	<i>N</i>	Specifies the module number.
	detail	(Optional) Specifies the display of detailed information for analysis.

Defaults Non-detailed results

Command Modes EXEC mode

Command History	Release	Modification
	12.2(18)EW	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines The **detail** keyword is intended for use by Cisco support personnel when analyzing failures.

Examples This example shows how to display the results of the bootup packet memory tests:

```
Switch# show diagnostic result module 1 test 2

Test results: (. = Pass, F = Fail, U = Untested)

    2) packet-memory-bootup -----> .
```

This example shows how to display detailed results from the bootup packet memory tests:

```
Switch# show diagnostic result module 2 test 2 detail

Test results: (. = Pass, F = Fail, U = Untested)
```

```
-----

    2) packet-memory-bootup -----> .

        Error code -----> 0 (DIAG_SUCCESS)
        Total run count -----> 0
        Last test execution time ----> n/a
        First test failure time ----> n/a
        Last test failure time ----> n/a
        Last test pass time -----> n/a
        Total failure count -----> 0
        Consecutive failure count ---> 0
packet buffers on free list: 64557 bad: 0 used for ongoing tests: 979
```

show diagnostic result module test 2

```
Number of errors found: 0
Cells with hard errors (failed two or more tests): 0
Cells with soft errors (failed one test, includes hard): 0
Suspect bad cells (uses a block that tested bad): 0
total buffers: 65536
bad buffers: 0 (0.0%)
good buffers: 65536 (100.0%)
Bootup test results:
No errors.
```

Related Commands

[diagnostic monitor action](#)
[show diagnostic result module test 3](#)

show diagnostic result module test 3

To display results from the ongoing packet memory test, use the **show diagnostic result module test 3** command. The output indicates whether the test passed, failed, or was not run.

show diagnostic result module *N* test 3 [detail]

Syntax Description	<i>N</i>	Specifies the module number.
	detail	(Optional) Specifies the display of detailed information for analysis.

Defaults Non-detailed results

Command Modes EXEC mode

Command History	Release	Modification
	12.2(18)EW	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines The **detail** keyword is intended for use by Cisco support personnel when analyzing failures.

Examples This example shows how to display results from the ongoing packet memory tests:

```
Switch# show diagnostic result module 1 test 3

Test results: (. = Pass, F = Fail, U = Untested)

    3) packet-memory-ongoing -----> .
```

This example shows how to display detailed results from the ongoing packet memory tests:

```
Switch# show diagnostic result module 1 test 3 detail

Test results: (. = Pass, F = Fail, U = Untested)
```

```
-----

    3) packet-memory-ongoing -----> .

        Error code -----> 0 (DIAG_SUCCESS)
        Total run count -----> 0
        Last test execution time ----> n/a
        First test failure time ----> n/a
        Last test failure time ----> n/a
        Last test pass time -----> n/a
        Total failure count -----> 0
        Consecutive failure count ---> 0
packet buffers on free list: 64557 bad: 0 used for ongoing tests: 979
```

■ show diagnostic result module test 3

```

Packet memory errors: 0 0
Current alert level: green
Per 5 seconds in the last minute:
  0 0 0 0 0 0 0 0 0 0
  0 0
Per minute in the last hour:
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
Per hour in the last day:
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0
Per day in the last 30 days:
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
Direct memory test failures per minute in the last hour:
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
Potential false positives: 0 0
  Ignored because of rx errors: 0 0
  Ignored because of cdm fifo overrun: 0 0
  Ignored because of oir: 0 0
  Ignored because isl frames received: 0 0
  Ignored during boot: 0 0
  Ignored after writing hw stats: 0 0
  Ignored on high gigaport: 0
Ongoing diag action mode: Normal
Last 1000 Memory Test Failures: v
Last 1000 Packet Memory errors:
First 1000 Packet Memory errors:

```

Related Commands

[diagnostic monitor action](#)
[show diagnostic result module test 2](#)

show dot1x

To display 802.1X statistics and operational status for the entire switch or for a specified interface, use the **show dot1x** command.

show dot1x [**interface** *interface-id*] | [**statistics** [**interface** *interface-id*]] | [**all**]

Syntax Description	
interface <i>interface-id</i>	(Optional) Displays the 802.1X status for the specified port.
statistics	(Optional) Displays 802.1X statistics for the switch or the specified interface.
all	(Optional) Displays per-interface 802.1X configuration information for all interfaces with a non-default 802.1X configuration.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(19)EW	Display enhanced to show the guest-VLAN value.

Usage Guidelines

If you do not specify an interface, global parameters and a summary are displayed. If you specify an interface, details for that interface are displayed.

If you specify the **statistics** keyword without the **interface** *interface-id* option, statistics are displayed for all interfaces. If you specify the **statistics** keyword with the **interface** *interface-id* option, statistics are displayed for the specified interface.

Expressions are case sensitive. For example, if you enter **exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples This is an example of output from the **show dot1x** privileged EXEC command:

```
Switch# show dot1x
Sysauthcontrol = Disabled
Dot1x Protocol Version = 1
Dot1x Oper Controlled Directions = Both
Dot1x Admin Controlled Directions = Both
Switch#
```

This example shows how to display 802.1x statistics for a specific port:

```
Switch# show dot1x interface fastethernet3/2

AuthSM State      = AUTHENTICATED(GUEST_VLAN)
BendSM State      = IDLE
PortStatus        = AUTHORIZED
MaxReq            = 2
MultiHosts        = Disabled
Port Control      = Auto
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds
Guest-Vlan        = 91
Switch#
```

**Note**

[Table2-12](#) provides a partial list of the displayed fields. The remaining fields in the display show internal state information. For a detailed description of these state machines and their settings, refer to the IEEE 802.1X specification.

Table2-12 show dot1x interface Field Description

Field	Description
PortStatus	Status of the port (authorized or unauthorized). The status of a port is displayed as authorized if the dot1x port-control interface configuration command is set to auto and has successfully completed authentication.
Port Control	Setting of the dot1x port-control interface configuration command.
MultiHosts	Setting of the dot1x multiple-hosts interface configuration command (allowed or disallowed).

This is an example of output from the **show dot1x statistics interface gigabitethernet1/1** command. [Table2-13](#) describes the fields in the display.

```
Switch# show dot1x statistics interface gigabitethernet1/1

PortStatistics Parameters for Dot1x
-----
TxReqId = 0      TxReq = 0      TxTotal = 0
RxStart = 0      RxLogoff = 0  RxRespId = 0  RxResp = 0
RxInvalid = 0    RxLenErr = 0  RxTotal = 0
RxVersion = 0    LastRxSrcMac 0000.0000.0000
Switch#
```

Table2-13 show dot1x statistics Field Descriptions

Field	Description
TxReq/TxReqId	Number of EAP-request/identity frames that have been sent.
TxTotal	Number of EAPOL frames of any type that have been sent.
RxStart	Number of valid EAPOL-start frames that have been received.
RxLogoff	Number of EAPOL-logoff frames that have been received.

Table2-13 show dot1x statistics Field Descriptions (continued)

Field	Description
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	Protocol version number carried in the most recently received EAPOL frame.
LastRxSrcMac	Source MAC address carried in the most recently received EAPOL frame.

Related Commands

[dot1x guest-vlan](#)
[dot1x max-reauth-req](#)
[dot1x port-control](#)

show environment

To display environment alarm, operational status, and the current reading for the chassis, use the **show environment** command.

```
show environment [alarm] | [status [chassis | fantray | powersupply | supervisor]] |
[temperature]
```

Syntax Description

alarm	(Optional) Specifies alarm status of the chassis.
status	(Optional) Specifies operational status information.
chassis	(Optional) Specifies operational status of the chassis.
fantray	(Optional) Specifies status of the fan tray, and shows fan tray power consumption.
powersupply	(Optional) Specifies status of the power supply.
supervisor	(Optional) Specifies status of the supervisor engine.
temperature	(Optional) Specifies current chassis temperature readings.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Support for the ability to display generic environment information with the show environment command was added.

Examples

This example shows how to display information about environment alarms, operational status, and the current temperature readings for the chassis:

```
Switch# show environment
no alarm

Chassis Temperature           = 32 degrees Celsius
Chassis Over Temperature Threshold = 75 degrees Celsius
Chassis Critical Temperature Threshold = 95 degrees Celsius

Power Supply Model No      Type      Fan Status      Sensor
-----
PS1   PWR-C45-1400AC    AC 1400W    good          good
PS2   none                --          --            --

Power Supply      Max      Min      Max      Min      Absolute
(Nos in Watts)   Inline  Inline  System  System  Maximum
-----
PS1                0        0      1360    1360    1400
PS2                --        --        --        --        --
```

```
Power supplies needed by system : 1
```

```
Chassis Type : WS-C4507R
```

```
Supervisor Led Color : Green
```

```
Fantray : good
```

```
Power consumed by Fantray : 50 Watts
```

This example shows how to display information about environment alarms:

```
Switch# show environment alarm
no alarm
Switch#
```

This example shows how to display information about power supplies, chassis type, and fan trays:

```
Switch# show environment status
```

Power Supply	Model No	Type	Status	Fan Sensor
PS1	PWR-C45-1400AC	AC 1400W	good	good
PS2	none	--	--	--

Power Supply (Nos in Watts)	Max Inline	Min Inline	Max System	Min System	Absolute Maximum
PS1	0	0	1360	1360	1400
PS2	--	--	--	--	--

```
Power supplies needed by system : 1
```

```
Chassis Type : WS-C4507R
```

```
Supervisor Led Color : Green
```

```
Fantray : good
```

```
Power consumed by Fantray : 50 Watts
```

```
Switch#
```

This example shows how to display information about the chassis:

```
Switch# show environment status chassis
Chassis Type : WS-C4006
Switch#
```

This example shows how to display information about the fan tray:

```
Switch# show environment status fantray
Fantray : good
Power consumed by Fantray : 50 Watts
Switch#
```

This example shows how to display information about the power supply:

```
Switch# show environment status powersupply
Power                               Fan
Supply Model No                    Type      Status   Sensor
-----
PS1   WS-X4008                      AC 400W   good     good
PS2   WS-X4008                      AC 400W   good     good
PS3   none                            --        --       --
Switch#
```

This example shows how to display information about the supervisor engine:

```
Switch# show environment status supervisor
Supervisor Led Color :Green
Switch#
```

This example shows how to display information about the temperature of the chassis:

```
Switch# show environment temperature
Chassis Temperature                = 32 degrees Celsius
Chassis Over Temperature Threshold = 75 degrees Celsius
Chassis Critical Temperature Threshold = 95 degrees Celsius
Switch#
```

show errdisable detect

To display error disable detection status, use the **show errdisable detect** command.

show errdisable detect

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(19)EW	Display includes the status of storm control.

Examples This example shows how to display error disable detection status:

```
Switch# show errdisable detect
ErrDisable Reason      Detection status
-----
udld                   Enabled
bpduguard              Enabled
security-violatio     Enabled
channel-misconfig     Disabled
psecure-violation     Enabled
vmps                   Enabled
pagp-flap              Enabled
dtp-flap               Enabled
link-flap              Enabled
l2ptguard              Enabled
gbic-invalid           Enabled
dhcp-rate-limit       Enabled
unicast-flood         Enabled
storm-control         Enabled
ilpower                Enabled
arp-inspection        Enabled
Switch#
```

Related Commands

- [errdisable detect](#)
- [errdisable recovery](#)
- [show interfaces status](#)

show errdisable recovery

To display error disable recovery timer information, use the **show errdisable recovery** command.

show errdisable recovery

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(19)EW	Display includes the status of storm control.

Examples This example shows how to display recovery timer information for error disable:

```
Switch# show errdisable recovery
ErrDisable Reason      Timer Status
-----
udld                   Disabled
bpduguard              Disabled
security-violatio     Disabled
channel-misconfig     Disabled
vmps                   Disabled
pagp-flap              Disabled
dtp-flap               Disabled
link-flap              Disabled
l2ptguard              Disabled
psecure-violation     Disabled
gbic-invalid           Disabled
dhcp-rate-limit       Disabled
unicast-flood         Disabled
storm-control         Disabled
arp-inspection        Disabled

Timer interval:30 seconds

Interfaces that will be enabled at the next timeout:

Interface      Errdisable reason      Time left(sec)
-----
Fa7/32         arp-inspect             13
```

Related Commands

- [errdisable detect](#)
- [errdisable recovery](#)
- [show interfaces status](#)

show etherchannel

To display EtherChannel information for a channel, use the **show etherchannel** command.

```
show etherchannel[channel-group] { port-channel | brief | detail | summary | port | load-balance
| protocol}
```

Syntax Description	
<i>channel-group</i>	(Optional) Number of the channel group; valid values are from 1 to 64.
port-channel	Displays port channel information.
brief	Displays a summary of EtherChannel information.
detail	Displays detailed EtherChannel information.
summary	Displays a one-line summary per channel group.
port	Displays EtherChannel port information.
load-balance	Displays load-balance information.
protocol	Displays the enabled protocol.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(13)EW	Support for LACP was added to this command.

Usage Guidelines If you do not specify a channel group, all channel groups are displayed.

In the output below, the Passive port list field is displayed for Layer 3 port channels only. This field means that the physical interface, 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).

Examples This example shows how to display port channel information for a specific group:

```
Switch# show etherchannel 1 port-channel
      Port-channels in the group:
      -----
Port-channel: Pol
-----
Age of the Port-channel   = 02h:35m:26s
Logical slot/port        = 10/1           Number of ports in agport = 0
GC                        = 0x00000000    HotStandBy port = null
Passive port list        = Fa5/4 Fa5/5
Port state                = Port-channel L3-Ag Ag-Not-Inuse
```

show etherchannel

```
Ports in the Port-channel:
Index  Load  Port
-----
Switch#
```

This example shows how to display load-balancing information:

```
Switch# show etherchannel load-balance
Source XOR Destination mac address
Switch#
```

This example shows how to display a summary of information for a specific group:

```
Switch# show etherchannel 1 brief
Group state = L3
Ports: 2 Maxports = 8
port-channels: 1 Max port-channels = 1
Switch#
```

This example shows how to display detailed information for a specific group:

```
Switch# show etherchannel 1 detail
Group state = L3
Ports: 2 Maxports = 8
Port-channels: 1 Max Port-channels = 1
                Ports in the group:
                -----
Port: Fa5/4
-----

Port state      = EC-Enbld Down Not-in-Bndl Usr-Config
Channel group = 1          Mode = Desirable      Gcchange = 0
Port-channel   = null      GC   = 0x00000000      Pseudo-agport = Po1
Port indx      = 0          Load = 0x00

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.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Local information:

Port      Flags State   Timers  Hello  Partner  PAgP    Learning  Group
Fa5/4     d    U1/S1    1s      0      0        128     Any       0

Age of the port in the current state: 02h:33m:14s
Port: Fa5/5
-----

Port state      = EC-Enbld Down Not-in-Bndl Usr-Config
Channel group = 1          Mode = Desirable      Gcchange = 0
Port-channel   = null      GC   = 0x00000000      Pseudo-agport = Po1
Port indx      = 0          Load = 0x00

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.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Local information:

Port      Flags State   Timers  Hello  Partner  PAgP    Learning  Group
Fa5/5     d    U1/S1    1s      0      0        128     Any       0
```



```

Age of the port in the current state: 02h:33m:17s
Port-channels in the group:
-----

Port-channel: Po1
-----
Age of the Port-channel = 02h:33m:52s
Logical slot/port = 10/1          Number of ports in agport = 0
GC = 0x00000000          HotStandBy port = null
Passive port list = Fa5/4 Fa5/5
Port state = Port-channel L3-Ag Ag-Not-Inuse

```

Ports in the Port-channel:

```

Index  Load  Port
-----
Switch#

```

This example shows how to display a one-line summary per channel group:

```

Switch# show etherchannel summary
U-in use I-in port-channel S-suspended D-down i-stand-alone d-default

Group Port-channel Ports
-----
1      Po1(U)        Fa5/4(I) Fa5/5(I)
2      Po2(U)        Fa5/6(I) Fa5/7(I)
Switch#

```

This example shows how to display EtherChannel port information for all ports and all groups:

```

Switch# show etherchannel port
Channel-group listing:
-----

Group: 1
-----
Ports in the group:
-----

Port: Fa5/4
-----
Port state = EC-Enbl'd Down Not-in-Bndl Usr-Config
Channel group = 1          Mode = Desirable          Gcchange = 0
Port-channel = null       GC = 0x00000000          Pseudo-agport = Po1
Port indx = 0              Load = 0x00

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.
Timers: H - Hello timer is running.        Q - Quit timer is running.
      S - Switching timer is running.      I - Interface timer is running.

Local information:
Port      Flags State  Timers  Hello  Partner  PAgP  Learning  Group
Fa5/4    d     U1/S1  1s      0      0        128   Any       0

Age of the port in the current state: 02h:40m:35s
Port: Fa5/5
-----

Port state = EC-Enbl'd Down Not-in-Bndl Usr-Config
Channel group = 1          Mode = Desirable          Gcchange = 0
Port-channel = null       GC = 0x00000000          Pseudo-agport = Po1
Port indx = 0              Load = 0x00

```

show etherchannel

```

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.
Timers: H - Hello timer is running.       Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

```

<...output truncated...>

Switch#

This example shows how to display the protocol enabled:

```

Switch# show etherchannel protocol
          Channel-group listing:
          -----

Group: 12
-----
Protocol:  PAgP

Group: 24
-----
Protocol:  - (Mode ON)
Switch#

```

Related Commands

[channel-group](#)
[interface port-channel](#)

show flowcontrol

To display the per-interface status and statistics related to flow control, use the **show flowcontrol** command.

show flowcontrol [**module** *slot* | **interface** *interface*]

Syntax Description	module <i>slot</i>	(Optional) Limits the display to interfaces on a specific module.
	interface <i>interface</i>	(Optional) Displays the status on a specific interface.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Table 2-14 describes the fields in the **show flowcontrol** command output.

Table2-14 show flowcontrol Command Output

Field	Description
Port	Module and port number.
Send-Flowcontrol-Admin	Flow-control administration. Possible settings: on indicates the local port sends flow control to the far end; off indicates the local port does not send flow control to the far end; desired indicates the local end sends flow control to the far end if the far end supports it.
Send-Flowcontrol-Oper	Flow-control operation. Possible setting: disagree indicates the two ports could not agree on a link protocol.
Receive-Flowcontrol-Admin	Flow-control administration. Possible settings: on indicates the local port requires the far end to send flow control; off indicates the local port does not allow the far end to send flow control; desired indicates the local end allows the far end to send flow control.
Receive-Flowcontrol-Oper	Flow-control operation. Possible setting: disagree indicates the two ports could not agree on a link protocol.
RxPause	Number of pause frames received.
TxPause	Number of pause frames transmitted.

Examples

This example shows how to display flow control status on all the gigabit interfaces:

```
Switch# show flowcontrol
Port      Send FlowControl  Receive FlowControl  RxPause TxPause
         admin   oper    admin   oper
-----
Gi1/1    desired  off     off     off     0       0
Gi1/2    on       disagree on     on     0       0
Gi3/1    on       on      on     on     0       0
Gi3/2    desired  off     off     off     0       0
Gi3/3    desired  off     off     off     0       0
Gi3/4    off      off     on     on     0       0
Gi3/5    desired  off     off     off     0       0
Gi3/6    desired  off     off     off     0       0
Switch#
```

This example shows how to display the flow control status on module 1:

```
Switch# show flowcontrol module 1
Port      Send FlowControl  Receive FlowControl  RxPause TxPause
         admin   oper    admin   oper
-----
Gi1/1    desired  off     off     off     0       0
Gi1/2    on       disagree on     on     0       0
Switch#
```

This example shows how to display the flow control status on interface 3/4:

```
Switch# show flowcontrol interface gigabitethernet 3/4
Port      Send FlowControl  Receive FlowControl  RxPause TxPause
         admin   oper    admin   oper
-----
Gi3/4    off      off     on     on     0       0
Switch#
```

Related Commands

[flowcontrol](#)
[show interfaces status](#)

show idprom

To display IDPROMs for the chassis, supervisor engine, module, power supplies, fan trays, clock module, and multiplexor (mux) buffer, use the **show idprom** command.

```
show idprom { all | chassis | module [mod] | interface int_name | supervisor | power-supply
  number | fan-tray }
```

Syntax Description		
	all	Displays information for all IDPROMs.
	chassis	Displays information for chassis IDPROMs.
	module	Displays information for module IDPROMs.
	<i>mod</i>	(Optional) Specifies the module name.
	interface <i>int_name</i>	Displays information for GBIC or SFP IDPROMs.
	supervisor	Displays information for supervisor engine IDPROMs.
	power-supply <i>number</i>	Displays information for power supply IDPROMs.
	fan-tray	Displays information for the fan tray IDPROMs.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for the power-supply , fan-tray , clock-module , and mux-buffer keywords was added.
	12.1(13)EW	Support for interface keyword was added.
	12.2(18)EW	Enhanced the show idprom interface output to include the hexadecimal display of the GBIC/SFP SEEPROM contents.

Usage Guidelines When you enter the **show idprom interface** command, the output lines for Calibration type and Rx (receive) power measurement may not be displayed for all GBICs.

Examples This example shows how to display IDPROM information for module 4:

```
Switch# show idprom module 4
Module 4 Idprom:
Common Block Signature = 0xABAB
Common Block Version = 1
Common Block Length = 144
Common Block Checksum = 4199
Idprom Size = 256
Block Count = 2
```

```

FRU Major Type = 0x4201
FRU Minor Type = 303
OEM String = Cisco Systems, Inc.
Product Number = WS-X4306
Serial Number = 00000135
Part Number = <tbid>
Hardware Revision = 0.2
Manufacturing Bits = 0x0000
Engineering Bits = 0x0000
Snmp OID = 0.0.0.0.0.0.0
Power Consumption = 0
RMA Failure Code = 0 0 0 0
Linecard Block Signature = 0x4201
Linecard Block Version = 1
Linecard Block Length = 24
Linecard Block Checksum = 658
Feature Bits = 0x0000000000000000
Card Feature Index = 50
MAC Base = 0010.7bab.9830
MAC Count = 6
Switch#

```

This example shows how to display IDPROM information for the GBICs on the Gigabit Ethernet interface 1/2:

```

Switch# show idprom interface GigabitEthernet 1/2
GBIC Serial EEPROM Contents:
Common Block:
Identifier          = GBIC [0x1]
Extended Id         = Not specified/compliant with defined MOD_DEF [0x0]
Connector           = SC connector [0x1]
Transceiver
  Speed              = Not available [0x0]
  Media               = Not available [0x0]
  Technology          = Not available [0x0]
  Link Length        = Not available [0x0]
  GE Comp Codes       = Not available [0x0]
  SONET Comp Codes   = Not available [0x0]
Encoding            = 8B10B [0x1]
BR, Nominal          = 1300000000 MHz
Length(9u) in km    = GBIC does not support single mode fibre, or the length
                    must be determined from the transceiver technology.
Length(9u)           = > 25.4 km
Length(50u)          = GBIC does not support 50 micron multi-mode fibre, or the
                    length must be determined from the transceiver technology.
Length(62.5u)        = GBIC does not support 62.5 micron multi-mode fibre, or
                    the length must be determined from transceiver technology.
Length(Copper)       = GBIC does not support copper cables, or the length must
                    be determined from the transceiver technology.
Vendor name          = CISCO-FINISAR
Vendor OUI           = 36965
Vendor Part No.      = FTR-0119-CSC
Vendor Part Rev.     = B
Wavelength           = Not available
CC_BASE              = 0x1A

Extended ID Fields
Options              = Loss of Signal implemented TX_FAULT signal implemented TX_DISABLE is
                    implemented and disables the serial output [0x1A]
BR, max              = Unspecified
BR, min              = Unspecified
Vendor Serial No.    = K1273DH
Date code            = 030409
Diag monitoring       = Implemented

```

```

Calibration type = Internal
Rx pwr measuremnt = Optical Modulation Amplitude (OMA)
Address change = Required
CC_EXT = 0xB2

Vendor Specific ID Fields:
20944D30 29 00 02 80 22 33 38 3D C7 67 83 E8 DF 65 6A AF )..."38=Gg^Ch_ej/
20944D40 1A 80 ED 00 00 00 00 00 00 00 00 00 38 23 3C 1B .....8#<.

SEEPROM contents (hex) size 128:
0x0000 01 00 01 00 00 00 00 00 00 00 01 0D 00 00 FF .....
0x0010 00 00 00 00 43 49 53 43 4F 2D 46 49 4E 49 53 41 ....CISCO-FINISA
0x0020 52 20 20 20 00 00 00 90 65 46 54 52 2D 30 31 31 39 R ..^PeFTR-0119
0x0030 2D 43 53 43 20 20 20 20 42 20 20 20 00 00 00 1A -CSC B ....
0x0040 00 1A 00 00 4B 31 32 37 33 44 48 20 20 20 20 20 ....K1273DH
0x0050 20 20 20 20 30 33 30 34 30 39 20 20 64 00 00 B2 030409 d..2
0x0060 29 00 02 80 22 33 38 3D C7 67 83 E8 DF 65 6A AF )..^@"38=Gg^C._ej.
0x0070 1A 80 ED 00 00 00 00 00 00 00 00 00 38 23 3C 1B .^@m.....8#<.
Switch#

```

This example shows how to display IDPROM information for the supervisor engine:

```

Switch# show idprom supervisor
Supervisor Idprom:
Common Block Signature = 0xABAB
Common Block Version = 1
Common Block Length = 144
Common Block Checksum = 4153
Idprom Size = 256
Block Count = 2
FRU Major Type = 0x4101
FRU Minor Type = 333
OEM String = Cisco Systems, Inc.
Product Number = WS-X4014
Serial Number = JAB05320CCE
Part Number = 73-6854-04
Part Revision = 05
Manufacturing Deviation String = 0
Hardware Revision = 0.4
Manufacturing Bits = 0x0000
Engineering Bits = 0x0000
Snmp OID = 0.0.0.0.0.0.0.0
Power Consumption = 0
RMA Failure Code = 0 0 0 0
Supervisor Block Signature = 0x4101
Supervisor Block Version = 1
Supervisor Block Length = 24
Supervisor Block Checksum = 548
Feature Bits = 0x0000000000000000
Card Feature Index = 95
MAC Base = 0007.0ee5.2a44
MAC Count = 2
Switch#

```

This example shows how to display IDPROM information for the chassis:

```

Switch# show idprom chassis
Chassis Idprom:
Common Block Signature = 0xABAB
Common Block Version = 1
Common Block Length = 144
Common Block Checksum = 4285
Idprom Size = 256

```

```

Block Count = 2
FRU Major Type = 0x4001
FRU Minor Type = 24
OEM String = Cisco Systems, Inc.
Product Number = WS-C4006
Serial Number = FOX04473737
Part Number = 73-4289-02
Part Revision = 02
Manufacturing Deviation String = 0x00
Hardware Revision = 0.2
Manufacturing Bits = 0x0000
Engineering Bits = 0x0000
Snmp OID = 0.0.0.0.0.0.0
Chassis Block Signature = 0x4001
Chassis Block Version = 1
Chassis Block Length = 22
Chassis Block Checksum = 421
Feature Bits = 0x0000000000000000
MAC Base = 0004.dd42.2600
MAC Count = 1024
Switch#

```

This example shows how to display IDPROM information for power supply 1:

```

Switch# show idprom power-supply 1
Power Supply 0 Idprom:
Common Block Signature = 0xABAB
Common Block Version = 1
Common Block Length = 144
Common Block Checksum = 10207
Idprom Size = 256
Block Count = 1
FRU Major Type = 0xAB01
FRU Minor Type = 8224
OEM String = Cisco Systems, Inc.
Product Number = WS-CAC-1440W
Serial Number = ACP05180002
Part Number = 34-XXXX-01
Part Revision = A0
Manufacturing Deviation String =
Hardware Revision = 1.1
Manufacturing Bits = 0x0000
Engineering Bits = 0x3031
Snmp OID = 9.12.3.65535.65535.65535.65535.65535
Power Consumption = -1
RMA Failure Code = 255 255 255 255
Power Supply Block Signature = 0xFFFF
PowerSupply Block Version = 255
PowerSupply Block Length = 255
PowerSupply Block Checksum = 65535
Feature Bits = 0x00000000FFFFFFFF
Current @ 110V = -1
Current @ 220V = -1
StackMIB OID = 65535
Switch#

```

This example shows how to display IDPROM information for the fan tray:

```

Switch# show idprom fan-tray
Fan Tray Idprom :
Common Block Signature = 0xABAB
Common Block Version = 1
Common Block Length = 144
Common Block Checksum = 19781

```



```
Idprom Size = 256
Block Count = 1
FRU Major Type = 0x4002
FRU Minor Type = 0
OEM String = "Cisco Systems"
Product Number = WS-X4502-fan
Serial Number =
Part Number =
Part Revision =
Manufacturing Deviation String =
Hardware Revision = 0.1
Manufacturing Bits = 0xFFFF
Engineering Bits = 0xFFFF
Snmp OID = 65535.65535.65535.65535.65535.65535.65535.65535
Power Consumption = -1
RMA Failure Code = 255 255 255 255
Switch#
```

show interfaces

To display traffic on a specific interface, use the **show interfaces** command.

```
show interfaces [{ FastEthernet mod/interface-number } | { GigabitEthernet
mod/interface-number } | { null interface-number } | vlan vlan_id } | status ]]
```

Syntax Description

FastEthernet <i>mod/interface-number</i>	(Optional) Specifies the Fast Ethernet module and interface.
GigabitEthernet <i>mod/interface-number</i>	(Optional) Specifies the Gigabit Ethernet module and interface.
null <i>interface-number</i>	(Optional) Specifies the null interface; the valid value is 0.
vlan <i>vlan_id</i>	(Optional) Specifies the VLAN; valid values are from 1 to 4094.
status	(Optional) Displays status information.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Support for extended VLAN addresses was added.

Usage Guidelines

Statistics are collected on a per-VLAN basis for Layer 2-switched packets and Layer 3-switched packets. Statistics are available for both unicast and multicast. The Layer 3-switched packet counts are available for both ingress and egress directions. The per-VLAN statistics are updated every 5 seconds.

In some cases, you might see a difference in the duplex mode displayed between the **show interfaces** command and the **show running-config** commands. The duplex mode displayed in the **show interfaces** command is the actual duplex mode the interface is running. The **show interfaces** command shows the operating mode for an interface, while the **show running-config** command shows the configured mode for an interface.

If you do not enter any keywords, all counters for all modules are displayed.

Examples

This example shows how to display traffic for a specific interface:

```
Switch# show interfaces GigabitEthernet 2/5
GigabitEthernet9/5 is up, line protocol is up
Hardware is C4k 1000Mb 802.3, address is 0001.64f8.3fa5 (bia 0001.64f8.3fa5)
Internet address is 172.20.20.20/24
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
```

```

Full-duplex, 1000Mb/s
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output never, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 1000 bits/sec, 2 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
L2 Switched: ucast: 8199 pkt, 1362060 bytes - mcast: 6980 pkt, 371952 bytes
L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast
L3 out Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes
300114 packets input, 27301436 bytes, 0 no buffer
Received 43458 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 input packets with dribble condition detected
15181 packets output, 1955836 bytes, 0 underruns
0 output errors, 0 collisions, 3 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
Switch#

```

This example shows how to display status information for Gigabit Ethernet interface 1/2:

```

Switch# show interfaces Gi1/2 status
Port      Name      Status      Vlan      Duplex  Speed Type
Gi1/2                    notconnect  1         auto     1000 1000-XWDM-RXONLY
Switch#

```

show interfaces capabilities

To display the interface capabilities for an interface or for all the interfaces on a switch, use the **show interfaces capabilities** command.

show interfaces capabilities [{**module** *mod*}]

show interfaces [*interface interface-number*] **capabilities**

Syntax Description

module <i>mod</i>	(Optional) Keyword and variable to display information for the specified module only.
<i>interface</i>	(Optional) Specifies the interface type. Valid values are fastethernet , gigabitethernet , and port-channel .
<i>interface-number</i>	(Optional) Specifies the port number.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The *interface-number* variable designates the module and port number. Valid values for *interface-number* depend on the chassis and module used. For example, if you have a 48-port 10/100-Mbps Fast Ethernet RJ-21 (telco connector) switching module installed in a Catalyst 4507 chassis, valid values for the slot number are from 2 to 13 and valid values for the port number are 1 to 48.

Examples

This example shows how to display interface capabilities for a module:

```
Router# show interfaces capabilities module 1
GigabitEthernet1/1
  Model: WS-X4516-Gbic
  Type: Unsupported GBIC
  Speed: 1000
  Duplex: full
  Trunk encap. type: 802.1Q, ISL
  Trunk mode: on, off, desirable, nonegotiate
  Channel: yes
  Broadcast suppression: percentage(0-100), hw
  Flowcontrol: rx-(off, on, desired), tx-(off, on, desired)
  VLAN Membership: static, dynamic
  Fast Start: yes
  Queuing: rx-(N/A), tx-(4q1t, Sharing/Shaping)
  CoS rewrite: yes
  ToS rewrite: yes
```

```

Inline power:          no
SPAN:                  source/destination
UDLD                   yes
Link Debounce:        no
Link Debounce Time:   no
Port Security         yes
Dot1x                  yes
GigabitEthernet1/2
Model:                 WS-X4516-Gbic
Type:                  Unsupported GBIC
Speed:                 1000
Duplex:                full
Trunk encap. type:    802.1Q,ISL
Trunk mode:           on,off,desirable,nonegotiate
Channel:               yes
Broadcast suppression:percentage(0-100), hw
Flowcontrol:          rx-(off,on,desired),tx-(off,on,desired)
VLAN Membership:      static, dynamic
Fast Start:           yes
Queuing:               rx-(N/A), tx-(4q1t, Sharing/Shaping)
CoS rewrite:          yes
ToS rewrite:          yes
Inline power:          no
SPAN:                  source/destination
UDLD                   yes
Link Debounce:        no
Link Debounce Time:   no
Port Security         yes
Dot1x                  yes
Router#

```

This example shows how to display interface capabilities for interface gi1/1:

```

Switch# show interface gigabitethernet1/1 capabilities
GigabitEthernet1/1
Model:                 WS-X4014-Gbic
Type:                  No Gbic
Speed:                 1000
Duplex:                full
Trunk encap. type:    802.1Q,ISL
Trunk mode:           on,off,desirable,nonegotiate
Channel:               yes
Broadcast suppression:percentage(0-100), hw
Flowcontrol:          rx-(off,on,desired),tx-(off,on,desired)
VLAN Membership:      static, dynamic
Fast Start:           yes
Queuing:               rx-(N/A), tx-(4q1t, Sharing/Shaping)
CoS rewrite:          yes
ToS rewrite:          yes

Inline power:          no
SPAN:                  source/destination
UDLD                   yes
Link Debounce:        no
Link Debounce Time:   no
Port Security         yes
Dot1x                  yes
MTU Supported:        jumbo frames, baby giants
Switch#

```

This example shows how to display interface capabilities for interface fa3/1:

```
Switch#show interface fastethernet3/1 capabilities
FastEthernet3/1
  Model:                WS-X4148-RJ-RJ-45
  Type:                 10/100BaseTX
  Speed:               10,100,auto
  Duplex:              half,full,auto
  Trunk encap. type:   802.1Q,ISL
  Trunk mode:          on,off,desirable,nonegotiate
  Channel:             yes
  Broadcast suppression:percentage(0-100), sw
  Flowcontrol:         rx-(none),tx-(none)
  VLAN Membership:    static, dynamic
  Fast Start:         yes
  Queuing:             rx-(N/A), tx-(4q1t, Shaping)
  CoS rewrite:        yes
  ToS rewrite:        yes
  Inline power:        no
  SPAN:               source/destination
  UDLD:               yes
  Link Debounce:      no
  Link Debounce Time: no
  Port Security:      yes
  Dot1x:              yes
  MTU Supported:      no jumbo frames, baby giants
Switch#
```

Related Commands [show interfaces counters](#)

show interfaces counters

To display traffic on the physical interface, use the **show interfaces counters** command.

show interfaces counters [**all** | **detail** | **errors** | **storm-control** | **trunk**] [**module** *mod*]

Syntax Description	
all	(Optional) Displays all interface counters including errors, trunk, and detail.
detail	(Optional) Displays detailed interface counters.
errors	(Optional) Displays interface error counters.
storm-control	(Optional) Displays the number of packets discarded due to suppression on the interface.
trunk	(Optional) Displays interface trunk counters.
module <i>mod</i>	(Optional) Limits the display to interfaces on a specific module.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(19)EW	Support for storm control.
	12.2(18)EW	Support for the display of total suppression discards.

Usage Guidelines If you do not enter any keywords, all counters for all modules are displayed.
The display for the **storm-control** keyword includes suppressed multicast bytes.

Examples This example shows how to display error counters for a specific module:

```
Switch# show interfaces counters errors module 1
```

```
Port          Align-Err    FCS-Err    Xmit-Err    Rcv-Err    UnderSize
Gi1/1          0            0          0           0          0
Gi1/2          0            0          0           0          0

Port          Single-Col  Multi-Col  Late-Col  Excess-Col  Carri-Sen    Runts    Giants
Gi1/1          0          0          0         0           0           0        0
Gi1/2          0          0          0         0           0           0        0
Switch#
```

This example shows how to display traffic seen by a specific module:

```
Switch# show interfaces counters module 1

Port          InOctets  InUcastPkts  InMcastPkts  InBcastPkts
Gi1/1         0         0             0             0
Gi1/2         0         0             0             0

Port          OutOctets  OutUcastPkts  OutMcastPkts  OutBcastPkts
Gi1/1         0         0             0             0
Gi1/2         0         0             0             0
Switch#
```

This example shows how to display trunk counters for a specific module:

```
Switch# show interfaces counters trunk module 1

Port          TrunkFramesTx  TrunkFramesRx  WrongEncap
Gi1/1         0              0              0
Gi1/2         0              0              0
Switch#
```

This example shows how to display the number of packets discarded due to suppression:

```
Switch# show interfaces counters storm-control

Multicast Suppression : Enabled

Port          BcastSuppLevel  TotalSuppressionDiscards
Fa5/35       10.00%          6278550
Switch#
```

Related Commands [show interfaces capabilities](#)

show interfaces description

To display a description and status of an interface, use the **show interfaces description** command.

show interfaces [*interface*] **description**

Syntax Description	<i>interface</i> (Optional) Type of interface.
---------------------------	--

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples	This example shows how to display information for all interfaces:
-----------------	---

```
Switch# show interfaces description
Interface Status      Protocol Description
PO0/0     admin down    down    First interface
PO0/1     admin down    down
Gig1/1    up            up      GigE to server farm
Switch#
```

Related Commands	description (refer to Cisco IOS documentation)
-------------------------	---

show interfaces link

To display how long a cable has been disconnected from an interface, use the **show interfaces link** command:

```
show interfaces link [module mod_num]
```

Syntax Description	module <i>mod_num</i> (Optional) Limits the display to interfaces on a module.
---------------------------	---

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	If the interface state is up, the command displays 0:00. If the interface state is down, the time (in hours, minutes, and seconds) is displayed.
-------------------------	--

Examples	This example shows how to display active link-level information:
-----------------	--

```
Switch# show interfaces link

Port      Name           Down Time
-----
Gi1/1          00:00:00
Gi1/2          00:00:00
Gi3/1          00:00:00
Gi3/2          00:00:00
Fa4/1          00:00:00
Fa4/2          00:00:00
Fa4/3          00:00:00
Fa4/4          00:00:00
```

This example shows how to display inactive link-level information:

```
Switch# show interfaces link

Port      Name           Down Time
-----
Gi3/4          1 minute 28 secs
Gi3/5          1 minute 28 secs
Gi3/6          1 minute 28 secs
Gi4/1          1 minute 28 secs
```

In this example, the cable has been disconnected from the port for 1 minute and 28 seconds.

show interfaces mtu

To display the maximum transmission unit (MTU) size of all the physical interfaces and SVIs on the switch, use the **show interfaces mtu** command.

show interfaces mtu [**module** *mod*]

Syntax Description	module <i>mod</i> (Optional) Limits the display to interfaces on a specific module.
---------------------------	--

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples	This example shows how to display the MTU size for all interfaces on module 1:
-----------------	--

```
Switch> show interfaces mtu module 1

Port      Name           MTU
Gi1/1     Gi1/1          1500
Gi1/2     Gi1/2          1500
Switch>
```

Related Commands	mtu
-------------------------	---------------------

show interfaces private-vlan mapping

To display PVLAN mapping information for VLAN SVIs, use the **show interface private-vlan mapping** command.

show interface private-vlan mapping [active]

Syntax Description	active (Optional) Displays active interfaces only.
---------------------------	---

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	This command displays SVI information only.
-------------------------	---

Examples	This example shows how to display PVLAN mapping information:
-----------------	--

```
Switch# show interface private-vlan mapping
Interface Secondary VLAN Type
-----
vlan2      301          isolated
vlan2      302          isolated
Switch#
```

Related Commands	private-vlan private-vlan mapping
-------------------------	--

show interfaces status

To display interface status or a list of interfaces in error-disabled state, use the **show interfaces status** command.

show interfaces status [err-disabled]

Syntax Description	err-disabled (Optional) Displays interfaces in error-disabled state.				
Defaults	This command has no default settings.				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(8a)EW</td> <td>Support for this command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Release	Modification				
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.				

Examples

This example shows how to display the status of all interfaces:

```
Switch# show interfaces status

Port      Name                Status      Vlan      Duplex Speed Type
Gi1/1     Gi1/1               disabled    routed    full   1000 missing
Gi1/2     Gi1/2               notconnect  1         full   1000 unknown (4)
Fa5/1     Fa5/1               disabled    routed    auto   auto  10/100BaseTX
Fa5/2     Fa5/2               disabled    routed    auto   auto  10/100BaseTX
Fa5/3     Fa5/3               disabled    routed    auto   auto  10/100BaseTX
Fa5/4     Fa5/4               disabled    routed    auto   auto  10/100BaseTX
...
Fa5/15    Fa5/15              disabled    routed    auto   auto  10/100BaseTX
Fa5/16    Fa5/16              disabled    routed    auto   auto  10/100BaseTX
Fa5/17    Fa5/17              disabled    routed    auto   auto  10/100BaseTX
Switch#
```

This example shows how to display the status of interfaces in error-disabled state:

```
Switch# show interfaces status err-disabled

Port      Name                Status      Reason
Fa9/4     Fa9/4               notconnect  link-flap

informational error message when the timer expires on a cause
-----

5d04h:%PM-SP-4-ERR_RECOVER:Attempting to recover from link-flap err-disable state on Fa9/4
Switch#
```

Related Commands

[errdisable detect](#)
[show errdisable recovery](#)

show interfaces switchport

To display the administrative and operational status of a switching (nonrouting) port, use the **show interfaces switchport** command.

```
show interfaces [interface-id] switchport [module mod]
```

Syntax Description	
<i>interface-id</i>	(Optional) Specifies the interface ID for the physical port.
module <i>mod</i>	(Optional) Limits the display to interfaces on the specified module; valid values are from 1 to 6.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(19)EW	Support for per-interface display.
	12.2(18)EW	Support for displaying the status of native VLAN tagging in the command output.

Examples This example shows how to display switch-port information using the **begin** output modifier:

```
Switch# show interfaces switchport | include VLAN
Name: Fa5/6
Access Mode VLAN: 200 (VLAN0200)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: ALL
Switch#
```

This example shows how to display switch-port information for module 1:

```
Switch# show interfaces switchport module 1
Name:Gi1/1
Switchport:Enabled
Administrative Mode:dynamic auto
Operational Mode:down
Administrative Trunking Encapsulation:negotiate
Negotiation of Trunking:On
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Administrative private-vlan host-association:none
Administrative private-vlan mapping:none
Operational private-vlan:none
Trunking VLANs Enabled:ALL
Pruning VLANs Enabled:2-1001

Name:Gi1/2
Switchport:Enabled
```

```

Administrative Mode:dynamic auto
Operational Mode:down
Administrative Trunking Encapsulation:negotiate
Negotiation of Trunking:On
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Administrative private-vlan host-association:none
Administrative private-vlan mapping:none
Operational private-vlan:none
Trunking VLANs Enabled:ALL
Pruning VLANs Enabled:2-1001
Switch#

```

This example shows how to display the status of native VLAN tagging on the port:

```

Switch# show interfaces g1/2 switchport
Name: Gi1/2
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)
Native VLAN tagging: Disabled **
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Administrative private-vlan trunk Native VLAN tagging: Disabled
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled

```

Related Commands

[show interfaces capabilities](#)
[show interfaces counters](#)

show interfaces transceiver

To display diagnostic-monitoring data for all interfaces that have transceivers installed, use the **show interfaces transceiver** command.

```
show interfaces {{{int_name} transceiver {[detail]} | {transceiver [module mod] | detail [module mod]}}
```

Syntax Description	
<i>int_name</i>	(Optional) Specifies an interface.
detail	(Optional) Displays the calibrated values and the A2D readouts if the readout values differ from the calibrated values. Also displays the high-alarm, high-warning, low-warning, and low-alarm thresholds.
module <i>mod</i>	(Optional) Limits the display to interfaces on a specific module.

Defaults

The non-interface-specific versions of the **show interfaces transceiver** command are enabled by default.

The interface-specific versions of these commands are enabled by default if the specified interface has a transceiver (GBIC or SFP) configured for diagnostic monitoring, and the transceiver is in a module that supports diagnostic monitoring.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.2(18)EW	Support for the calibration keyword was withdrawn.

Usage Guidelines

The **show interfaces transceiver** command provides useful information under the following conditions:

- At least one transceiver is installed on a chassis that is configured for diagnostic monitoring.
- The transceiver is in a module that supports diagnostic monitoring.

If you notice that alarm and warning flags have been set on a transceiver, reenter the command to confirm.

Examples

This example shows how to display diagnostic monitoring data for all interfaces with transceivers installed on the switch:

```
Switch# show interfaces transceiver
If device is externally calibrated, only calibrated values are printed.
++ : high alarm, + : high warning, - : low warning, -- : low alarm.
NA or N/A: not applicable, Tx: transmit, Rx: receive.
mA: milliamperes, dBm: decibels (milliwatts).

      Port          Temperature  Voltage  Current  Optical  Optical
              (Celsius)  (Volts)  (mA)     Tx Power  Rx Power
              -----  -----  -----  -----  -----
Gi1/1          48.1         3.30     0.0      8.1 ++    N/A
Gi1/2          33.0         3.30     1.8     -10.0     -36.9
Gi2/1          43.7         5.03     50.6 +   -16.7 --   N/A
Gi2/2          39.2         5.02     25.7     0.8       N/A

Switch#
```



Note The value for Optical Tx Power (in dBm) equals ten times log (Tx Power in mW). If the Tx Power value is 3 mW, then the Optical Tx Power value equals $10 * \log(3)$, which equals $10 * .477$ or 4.77 dBm. The Optical Rx Power value behaves similarly. If Tx Power or Rx Power is zero, then its dBm value is undefined and is shown as N/A (not applicable).

This example shows how to display detailed diagnostic monitoring data, including calibrated values, alarm and warning thresholds, A2D readouts, and alarm and warning flags. The A2D readouts are reported separately in parentheses only if they differ from the calibrated values:

```
Switch# show interfaces transceiver detail
mA: milliamperes, dBm: decibels (milliwatts), NA or N/A: not applicable.
++ : high alarm, + : high warning, - : low warning, -- : low alarm.
A2D readouts (if they differ), are reported in parentheses.
The threshold values are calibrated.
```

Port	Temperature (Celsius)	High Alarm Threshold (Celsius)	High Warn Threshold (Celsius)	Low Warn Threshold (Celsius)	Low Alarm Threshold (Celsius)
Gi1/1	48.1	100.0	100.0	0.0	0.0
Gi1/2	34.9	100.0	100.0	0.0	0.0
Gi2/1	43.5	70.0	60.0	5.0	0.0
Gi2/2	39.1	70.0	60.0	5.0	0.0

Port	Voltage (Volts)	High Alarm Threshold (Volts)	High Warn Threshold (Volts)	Low Warn Threshold (Volts)	Low Alarm Threshold (Volts)
Gi1/1	3.30	6.50	6.50	N/A	N/A
Gi1/2	3.30	6.50	6.50	N/A	N/A
Gi2/1	5.03	5.50	5.25	4.75	4.50
Gi2/2	5.02	5.50	5.25	4.75	4.50

Port	Current (milliamperes)	High Alarm Threshold (mA)	High Warn Threshold (mA)	Low Warn Threshold (mA)	Low Alarm Threshold (mA)
Gi1/1	0.0	130.0	130.0	N/A	N/A
Gi1/2	1.7	130.0	130.0	N/A	N/A
Gi2/1	50.6 +	60.0	40.0	10.0	5.0
Gi2/2	25.8	60.0	40.0	10.0	5.0

show interfaces transceiver

Port	Optical Transmit Power (dBm)		High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi1/1	8.1	++	8.1	8.1	N/A	N/A
Gi1/2	-9.8		8.1	8.1	N/A	N/A
Gi2/1	-16.7 (-13.0)	--	3.4	3.2	-0.3	-0.5
Gi2/2	0.8 (5.1)		3.4	3.2	-0.3	-0.5

Port	Optical Receive Power (dBm)		High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi1/1	N/A		8.1	8.1	N/A	N/A
Gi1/2	-30.9		8.1	8.1	N/A	N/A
Gi2/1	N/A (-28.5)		5.9	-6.7	-28.5	-28.5
Gi2/2	N/A (-19.5)		5.9	-6.7	-28.5	-28.5

Switch#

This example shows how to display monitoring data for the interfaces that have transceivers installed on module 2:

Switch# show interfaces transceiver module 2

If device is externally calibrated, only calibrated values are printed.
 ++ : high alarm, + : high warning, - : low warning, -- : low alarm.
 NA or N/A: not applicable, Tx: transmit, Rx: receive.
 mA: milliamperes, dBm: decibels (milliwatts).

Port	Temperature (Celsius)	Voltage (Volts)	Current (mA)	Optical Tx Power (dBm)	Optical Rx Power (dBm)
Gi2/1	43.7	5.03	50.6 +	-16.7 --	N/A
Gi2/2	39.2	5.02	25.7	0.8	N/A

Switch#

This example shows how to display detailed monitoring data for the interfaces that have transceivers installed on module 2:

Switch# show interfaces transceiver detail module 2

mA: milliamperes, dBm: decibels (milliwatts), NA or N/A: not applicable.
 ++ : high alarm, + : high warning, - : low warning, -- : low alarm.
 A2D readouts (if they differ), are reported in parentheses.
 The threshold values are calibrated.

Port	Temperature (Celsius)	High Alarm Threshold (Celsius)	High Warn Threshold (Celsius)	Low Warn Threshold (Celsius)	Low Alarm Threshold (Celsius)
Gi2/1	43.5	70.0	60.0	5.0	0.0
Gi2/2	39.1	70.0	60.0	5.0	0.0

Port	Voltage (Volts)	High Alarm Threshold (Volts)	High Warn Threshold (Volts)	Low Warn Threshold (Volts)	Low Alarm Threshold (Volts)
Gi2/1	5.03	5.50	5.25	4.75	4.50
Gi2/2	5.02	5.50	5.25	4.75	4.50

Port	Current (milliamperes)		High Alarm Threshold (mA)	High Warn Threshold (mA)	Low Warn Threshold (mA)	Low Alarm Threshold (mA)
Gi2/1	50.6	+	60.0	40.0	10.0	5.0
Gi2/2	25.8		60.0	40.0	10.0	5.0

Port	Optical Transmit Power (dBm)		High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi2/1	-16.7 (-13.0)	--	3.4	3.2	-0.3	-0.5
Gi2/2	0.8 (5.1)		3.4	3.2	-0.3	-0.5

Port	Optical Receive Power (dBm)		High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi2/1	N/A (-28.5)		5.9	-6.7	-28.5	-28.5
Gi2/2	N/A (-19.5)		5.9	-6.7	-28.5	-28.5

Switch#

This example shows how to display monitoring data for the transceivers on interface Gi1/2:

```
Switch# show interfaces g1/2 transceiver
ITU Channel 23 (1558.98 nm),
Transceiver is externally calibrated.
If device is externally calibrated, only calibrated values are printed.
++ : high alarm, + : high warning, - : low warning, -- : low alarm.
NA or N/A: not applicable, Tx: transmit, Rx: receive.
mA: milliamperes, dBm: decibels (milliwatts).
```

Port	Temperature (Celsius)	Voltage (Volts)	Current (mA)	Optical Tx Power (dBm)	Optical Rx Power (dBm)
Gi2/1	43.7	5.03	50.6 +	-16.7 --	N/A

Switch#

This example shows how to display detailed monitoring data for the transceivers on interface Gi1/2:

```
Switch# show interfaces g1/2 transceiver detail
ITU Channel 23 (1558.98 nm),
Transceiver is externally calibrated.
mA: milliamperes, dBm: decibels (milliwatts), NA or N/A: not applicable.
++ : high alarm, + : high warning, - : low warning, -- : low alarm.
A2D readouts (if they differ), are reported in parentheses.
The threshold values are calibrated.
```

Port	Temperature (Celsius)	High Alarm Threshold (Celsius)	High Warn Threshold (Celsius)	Low Warn Threshold (Celsius)	Low Alarm Threshold (Celsius)
Gi2/1	43.5	70.0	60.0	5.0	0.0

Port	Voltage (Volts)	High Alarm Threshold (Volts)	High Warn Threshold (Volts)	Low Warn Threshold (Volts)	Low Alarm Threshold (Volts)
Gi2/1	5.03	5.50	5.25	4.75	4.50

■ show interfaces transceiver

Port	Current (milliamperes)		High Alarm Threshold (mA)	High Warn Threshold (mA)	Low Warn Threshold (mA)	Low Alarm Threshold (mA)
Gi2/1	50.6	+	60.0	40.0	10.0	5.0

Port	Optical Transmit Power (dBm)		High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi2/1	-16.7 (-13.0)	--	3.4	3.2	-0.3	-0.5

Port	Optical Receive Power (dBm)		High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi2/1	N/A (-28.5)		5.9	-6.7	-28.5	-28.5

Switch#

Related Commands

[show idprom](#)
[show interfaces status](#)

show interfaces trunk

To display port and module interface-trunk information, use the **show interfaces trunk** command.

show interfaces trunk [**module** *mod*]

Syntax Description	module <i>mod</i> (Optional) Limits the display to interfaces on the specified module; valid values are from 1 to 6.
---------------------------	---

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines If you do not specify a keyword, only information for trunking ports is displayed.

Examples This example shows how to display interface-trunk information for module 5:

```
Switch# show interfaces trunk module 5
```

Port	Mode	Encapsulation	Status	Native vlan
Fa5/1	routed	negotiate	routed	1
Fa5/2	routed	negotiate	routed	1
Fa5/3	routed	negotiate	routed	1
Fa5/4	routed	negotiate	routed	1
Fa5/5	routed	negotiate	routed	1
Fa5/6	off	negotiate	not-trunking	10
Fa5/7	off	negotiate	not-trunking	10
Fa5/8	off	negotiate	not-trunking	1
Fa5/9	desirable	n-isl	trunking	1
Fa5/10	desirable	negotiate	not-trunking	1
Fa5/11	routed	negotiate	routed	1
Fa5/12	routed	negotiate	routed	1
...				
Fa5/48	routed	negotiate	routed	1

Port	Vlans allowed on trunk
Fa5/1	none
Fa5/2	none
Fa5/3	none
Fa5/4	none
Fa5/5	none
Fa5/6	none
Fa5/7	none
Fa5/8	200
Fa5/9	1-1005

■ show interfaces trunk

```

Fa5/10    none
Fa5/11    none
Fa5/12    none

Fa5/48    none

Port      Vlans allowed and active in management domain
Fa5/1     none
Fa5/2     none
Fa5/3     none
Fa5/4     none
Fa5/5     none
Fa5/6     none
Fa5/7     none
Fa5/8     200
Fa5/9     1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005
Fa5/10    none
Fa5/11    none
Fa5/12    none

Fa5/48    none

Port      Vlans in spanning tree forwarding state and not pruned
Fa5/1     none
Fa5/2     none
Fa5/3     none
Fa5/4     none
Fa5/5     none
Fa5/6     none
Fa5/7     none
Fa5/8     200
Fa5/9     1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005
Fa5/10    none
Fa5/11    none

Fa5/48    none
Switch#

```

This example shows how to display trunking information for active trunking ports:

Switch# **show interfaces trunk**

```

Port      Mode           Encapsulation  Status        Native vlan
Fa5/9     desirable     n-isl          trunking      1

Port      Vlans allowed on trunk
Fa5/9     1-1005

Port      Vlans allowed and active in management domain
Fa5/9     1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005

Port      Vlans in spanning tree forwarding state and not pruned
Fa5/9     1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005
Switch#

```

show ip arp inspection

To show the status of dynamic ARP inspection for a specific range of VLANs, use the **show ip arp inspection** command.

```
show ip arp inspection {[statistics] vlan vlan-range | interfaces [interface-name]}
```

Syntax Description		
statistics	(Optional) Displays statistics for the following types of packets that have been processed by this feature: forwarded, dropped, MAC validation failure, and IP validation failure.	
vlan <i>vlan-range</i>	(Optional) When used with the statistics keyword, displays the statistics for the selected range of VLANs. Without the statistics keyword, displays the configuration and operating state of DAI for the selected range of VLANs.	
interfaces <i>interface-name</i>	(Optional) Displays the trust state and the rate limit of ARP packets for the provided interface. When the interface name is not specified, the command displays the trust state and rate limit for all applicable interfaces in the system.	

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to display the statistics of packets that have been processed by DAI for VLAN 3:

```
Switch# show ip arp inspection statistics vlan 3

Vlan      Forwarded      Dropped      DHCP Drops      ACL Drops
----      -
3         31753          102407        102407          0

Vlan      DHCP Permits    ACL Permits    Source MAC Failures
----      -
3         31753          0              0

Vlan      Dest MAC Failures  IP Validation Failures
----      -
3         0                0

Switch#
```

This example shows how to display the statistics of packets that have been processed by DAI for all active VLANs:

```
Switch# show ip arp inspection statistics
```

Vlan	Forwarded	Dropped	DHCP Drops	ACL Drops
1	0	0	0	0
2	0	0	0	0
3	68322	220356	220356	0
4	0	0	0	0
100	0	0	0	0
101	0	0	0	0
1006	0	0	0	0
1007	0	0	0	0

Vlan	DHCP Permits	ACL Permits	Source MAC Failures
1	0	0	0
2	0	0	0
3	68322	0	0
4	0	0	0
100	0	0	0
101	0	0	0
1006	0	0	0
1007	0	0	0

Vlan	Dest MAC Failures	IP Validation Failures
1	0	0
2	0	0
3	0	0
4	0	0
100	0	0
101	0	0
1006	0	0
1007	0	0

```
Switch#
```

This example shows how to display the configuration and operating state of DAI for VLAN 1:

```
Switch# show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation     : Disabled
```

Vlan	Configuration	Operation	ACL Match	Static ACL
1	Enabled	Active		

Vlan	ACL Logging	DHCP Logging
1	Deny	Deny

```
Switch#
```

This example shows how to display the trust state of interface Fa6/3:

```
Switch# show ip arp inspection interfaces fastEthernet 6/3
Interface      Trust State      Rate (pps)      Burst Interval
-----
Fa6/1          Untrusted        20              5
Switch#
```


This example shows how to display the trust state of the interfaces on the switch:

```
Switch# show ip arp inspection interfaces
Interface          Trust State      Rate (pps)
-----
Gi1/1              Untrusted       15
Gi1/2              Untrusted       15
Gi3/1              Untrusted       15
Gi3/2              Untrusted       15
Fa3/3              Trusted         None
Fa3/4              Untrusted       15
Fa3/5              Untrusted       15
Fa3/6              Untrusted       15
Fa3/7              Untrusted       15
Switch#
```

Related Commands

[arp access-list](#)
[clear ip arp inspection log](#)
[show ip arp inspection](#)

show ip arp inspection log

To show the status of the log buffer, use the **show ip arp inspection log** command.

show ip arp inspection log

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to display the current contents of the log buffer before and after the buffers are cleared:

```
Switch# show ip arp inspection log
Total Log Buffer Size : 10
Syslog rate : 0 entries per 10 seconds.
```

Interface	Vlan	Sender MAC	Sender IP	Num of Pkts
Fa6/3	1	0002.0002.0002	1.1.1.2	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.3	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.4	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.5	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.6	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.7	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.8	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.9	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.10	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.11	1(12:02:52 UTC Fri Apr 25 2003)
--	--	--	--	5(12:02:52 UTC Fri Apr 25 2003)

```
Switch#
```

This example shows how to clear the buffer with the **clear ip arp inspection log** command:

```
Switch# clear ip arp inspection log
Switch# show ip arp inspection log
Total Log Buffer Size : 10
Syslog rate : 0 entries per 10 seconds.
No entries in log buffer.
Switch#
```

Related Commands [arp access-list](#)
[clear ip arp inspection log](#)

show ip cef vlan

To view IP CEF VLAN interface status and configuration information and display the prefixes for a specific interface, use the **show ip cef vlan** command.

show ip cef vlan *vlan_num* [**detail**]

Syntax Description	
<i>vlan_num</i>	Number of the VLAN.
detail	(Optional) Displays detailed information.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to display the prefixes for a specific VLAN:

```
Switch# show ip cef vlan 1003
Prefix          Next Hop          Interface
0.0.0.0/0       172.20.52.1       FastEthernet3/3
0.0.0.0/32      receive
10.7.0.0/16     172.20.52.1       FastEthernet3/3
10.16.18.0/23   172.20.52.1       FastEthernet3/3
Switch#
```

This example shows how to display detailed IP CEF information for a specific VLAN:

```
Switch# show ip cef vlan 1003 detail
IP Distributed CEF with switching (Table Version 2364), flags=0x0
 1383 routes, 0 reresolve, 0 unresolved (0 old, 0 new)
 1383 leaves, 201 nodes, 380532 bytes, 2372 inserts, 989 invalidations
 0 load sharing elements, 0 bytes, 0 references
 universal per-destination load sharing algorithm, id 9B6C9823
 3 CEF resets, 0 revisions of existing leaves
 refcounts: 54276 leaf, 51712 node

Adjacency Table has 5 adjacencies
Switch#
```

show ip dhcp snooping

To display the DHCP snooping configuration, use the **show ip dhcp snooping** command.

show ip dhcp snooping

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to display the DHCP snooping configuration:

```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
5 10
Insertion of option 82 is enabled
Interface           Trusted      Rate limit (pps)
-----
FastEthernet6/11    no          10
FastEthernet6/36    yes         50
Switch#
```

Related Commands

- [ip dhcp snooping](#)
- [ip dhcp snooping information option](#)
- [ip dhcp snooping limit rate](#)
- [ip dhcp snooping trust](#)
- [ip dhcp snooping vlan](#)

show ip dhcp snooping binding

To display DHCP snooping binding entries, use the **show ip dhcp snooping binding** command.

```
show ip dhcp snooping binding [ip-address] [mac-address] [vlan vlan_num]
[interface interface_num]
```

Syntax Description		
<i>ip-address</i>	(Optional)	Specifies the binding entries IP address.
<i>mac-address</i>	(Optional)	Specifies the binding entries MAC address.
vlan <i>vlan_num</i>	(Optional)	Specifies a VLAN.
interface <i>interface_num</i>	(Optional)	Specifies an interface.

Defaults If no argument is specified the switch will display the entire DHCP snooping binding table.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines DHCP snooping is enabled on a VLAN only if both the global snooping and the VLAN snooping are enabled.

To configure a range of VLANs, use the optional *last_vlan* variable to specify the end of the VLAN range.

Examples This example shows how to display the DHCP snooping binding entries for a switch:

```
Switch# show ip dhcp snooping binding
```

```
MacAddress      IP Address      Lease (seconds)  Type              VLAN      Interface
-----
0000.0100.0201  10.0.0.1        1600             dhcp-snooping     100       FastEthernet3/1
Switch#
```

This example shows how to display a DHCP snooping binding entries IP address:

```
Switch# show ip dhcp snooping binding 172.100.101.102
```

```
MacAddress      IP Address      Lease (seconds)  Type              VLAN      Interface
-----
0000.0100.0201  172.100.101.102  1600             dhcp-snooping     100       FastEthernet3/1
Switch#
```

show ip dhcp snooping binding

This example shows how to display the DHCP snooping binding entries MAC address:

```
Switch# show ip dhcp snooping binding 55.5.5.2 0002.b33f.3d5f
```

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
00:02:B3:3F:3D:5F	55.5.5.2	492	dhcp-snooping	99	FastEthernet6/36

This example shows how to display the DHCP snooping binding entries MAC address for a specific VLAN:

```
Switch# show ip dhcp snooping binding 55.5.5.2 0002.b33f.3d5f vlan 99
```

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
00:02:B3:3F:3D:5F	55.5.5.2	479	dhcp-snooping	99	FastEthernet6/36

This example shows how to display dynamic DHCP snooping binding entries:

```
Switch# show ip dhcp snooping binding dynamic
```

MacAddress	IP Address	Lease (seconds)	Type	VLAN	Interface
0000.0100.0201	10.0.0.1	1600	dhcp-snooping	100	FastEthernet3/1

This example shows how to display DHCP snooping binding entries on VLAN 100:

```
Switch# show ip dhcp snooping binding vlan 100
```

MacAddress	IP Address	Lease (seconds)	Type	VLAN	Interface
0000.0100.0201	10.0.0.1	1600	dhcp-snooping	100	FastEthernet3/1

This example shows how to display DHCP snooping binding entries on Ethernet interface 0/1:

```
Switch# show ip dhcp snooping binding interface FastEthernet3/1
```

MacAddress	IP Address	Lease (seconds)	Type	VLAN	Interface
0000.0100.0201	10.0.0.1	1600	dhcp-snooping	100	FastEthernet3/1

[Table2-15](#) describes the fields in the **show ip dhcp snooping** command output.

Table2-15 show ip dhcp snooping Command Output

Field	Description
Mac Address	Client hardware MAC address
IP Address	Client IP address assigned from the DHCP server
Lease (seconds)	IP address lease time
Type	Binding type; statically configured from CLI or dynamically learned
VLAN	VLAN number of the client interface
Interface	Interface that connects to the DHCP client host

Related Commands

ip dhcp snooping information option
ip dhcp snooping limit rate
ip dhcp snooping trust
ip igmp snooping
ip igmp snooping vlan

show ip dhcp snooping database

To display the status of DHCP snooping database agent, use the **show ip dhcp snooping database** command.

show ip dhcp snooping database [detail]

Syntax Description	detail (Optional) Provides additional operating state and statistics information.
---------------------------	--

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(19)EW	Added support of state and statistics information.

Examples	This example shows how to display the DHCP snooping database:
-----------------	---

```
Switch# show ip dhcp snooping database
Agent URL :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts      :          0   Startup Failures :          0
Successful Transfers :          0   Failed Transfers :          0
Successful Reads    :          0   Failed Reads     :          0
Successful Writes   :          0   Failed Writes    :          0
Media Failures      :          0

Switch#
```

This example shows how to view additional operating statistics:

```
Switch# show ip dhcp snooping database detail
Agent URL : tftp://10.1.1.1/directory/file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 7 (00:00:07)
Abort Timer Expiry : Not Running
```



```

Last Succeeded Time : None
Last Failed Time : 17:14:25 UTC Sat Jul 7 2001
Last Failed Reason : Unable to access URL.

Total Attempts      :          21   Startup Failures :          0
Successful Transfers :          0   Failed Transfers :         21
Successful Reads    :          0   Failed Reads     :          0
Successful Writes   :          0   Failed Writes    :         21
Media Failures      :          0

First successful access: Read

Last ignored bindings counters :
Binding Collisions   :          0   Expired leases    :          0
Invalid interfaces   :          0   Unsupported vlans :          0
Parse failures       :          0

Last Ignored Time : None

Total ignored bindings counters:
Binding Collisions   :          0   Expired leases    :          0
Invalid interfaces   :          0   Unsupported vlans :          0
Parse failures       :          0

Switch#

```

Related Commands

[ip dhcp snooping](#)
[ip dhcp snooping database](#)
[ip dhcp snooping information option](#)
[ip dhcp snooping limit rate](#)
[ip dhcp snooping trust](#)
[ip dhcp snooping vlan](#)

show ip igmp interface

To view IP IGMP interface status and configuration information, use the **show ip igmp interface** command.

```
show ip igmp interface [FastEthernet slot/port | GigabitEthernet slot/port |
null interface-number | vlan vlan_id]
```

Syntax Description	FastEthernet <i>slot/port</i>	(Optional) Specifies the Fast Ethernet interface and the number of the slot and port.
	GigabitEthernet <i>slot/port</i>	(Optional) Specifies the Gigabit Ethernet interface and the number of the slot and port; valid values are from 1 to 9.
	null <i>interface-number</i>	(Optional) Specifies the null interface and the number of the interface; the only valid value is 0 .
	vlan <i>vlan_id</i>	(Optional) Specifies the VLAN and the number of the VLAN; valid values are from 1 to 4094.

Defaults If you do not specify a VLAN, information for VLAN 1 is shown.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Added support for extended VLAN addresses.

Usage Guidelines If you omit the optional arguments, the **show ip igmp interface** command displays information about all interfaces.

Examples This example shows how to view IGMP information for VLAN 200:

```
Switch# show ip igmp interface vlan 200
IGMP snooping is globally enabled
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 is running in IGMP-ONLY mode on this VLAN
Switch#
```

Related Commands [clear ip igmp group](#)
[show ip igmp snooping mrouter](#)

show ip igmp profile

To view all configured IGMP profiles or a specified IGMP profile, use the **show ip igmp profile** privileged EXEC command.

show ip igmp profile [*profile number*]

Syntax Description	<i>profile number</i> (Optional) IGMP profile number to be displayed; valid ranges are from 1 to 4294967295.
---------------------------	--

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(11b)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines If no profile number is entered, all IGMP profiles are displayed.

Examples This example shows how to display IGMP profile 40:

```
Switch# show ip igmp profile 40
IGMP Profile 40
  permit
  range 233.1.1.1 233.255.255.255
Switch#
```

This example shows how to display all IGMP profiles:

```
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
Switch#
```

Related Commands [ip igmp profile](#)

show ip igmp snooping

To display information on dynamically learned and manually configured VLAN switch interfaces, use the **show ip igmp snooping** command.

```
show ip igmp snooping [querier | group | mrouter] [vlan vlan_id] a.b.c.d [summary | sources | hosts] [count]
```

Syntax Description	
querier	(Optional) Specifies that the display will contain IP address and version information.
group	(Optional) Specifies that the display will list VLAN members sorted by group IP address.
mrouter	(Optional) Specifies that the display will contain information on dynamically learned and manually configured multicast switch interfaces.
vlan <i>vlan_id</i>	(Optional) Specifies a VLAN; valid values are from 1 to 1001 and from 1006 to 4094.
<i>a.b.c.d</i>	(Optional) Specifies a group address.
summary	(Optional) Specifies a display of detailed information for a v2 or v3 group.
sources	(Optional) Specifies a list of the source IPs for the specified group.
hosts	(Optional) Specifies a list of the host IPs for the specified group.
count	(Optional) Specifies a display of the total number of group addresses learned by the system on a global or per-VLAN basis.

Defaults This command has no default settings.

Command Modes EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(19)EW	Support for extended addressing was added.
	12.1(20)EW	Added support to display configuration state for IGMPv3 explicit host tracking.

Usage Guidelines You can also use the **show mac-address-table multicast** command to display entries in the MAC address table for a VLAN that has IGMP snooping enabled.

You can display IGMP snooping information for VLAN interfaces by entering the **show ip igmp snooping** command.

Examples

This example shows how to display the global snooping information on the switch:

```
Switch> show ip igmp snooping
Global IGMP Snooping configuration:
-----
IGMP snooping           : Enabled
IGMPv3 snooping        : Enabled
Report suppression     : Enabled
TCN solicit query      : Disabled
TCN flood query count   : 2

Vlan 1:
-----
IGMP snooping           : Enabled
IGMPv2 immediate leave : Disabled
Explicit host tracking  : Enabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode : IGMP_ONLY

Vlan 2:
-----
IGMP snooping           : Enabled
IGMPv2 immediate leave : Disabled
Explicit host tracking  : Enabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode : IGMP_ONLY
Switch>
```

This example shows how to display the snooping information on VLAN 2:

```
Switch> show ip igmp snooping vlan 2
Global IGMP Snooping configuration:
-----
IGMP snooping           : Enabled
IGMPv3 snooping        : Enabled
Report suppression     : Enabled
TCN solicit query      : Disabled
TCN flood query count   : 2

Vlan 2:
-----
IGMP snooping           : Enabled
IGMPv2 immediate leave : Disabled
Explicit host tracking  : Enabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode : IGMP_ONLY
Switch>
```

This example shows how to display IGMP querier information for all VLANs on a switch:

```
Switch# show ip igmp snooping querier
Vlan      IP Address      IGMP Version      Port
-----
2         10.10.10.1      v2                 Router
3         172.20.50.22   v3                 Fa3/15
Switch>
```

■ show ip igmp snooping

This example shows how to display IGMP querier information for VLAN 5 when running IGMPv2:

```
Switch# show ip igmp snooping querier vlan 5
IP address           :5.5.5.10
IGMP version         :v2
Port                 :Fa3/1
Max response time    :10s
Switch>
```

This example shows how to display IGMP querier information for VLAN 5 when running IGMPv3:

```
Switch# show ip igmp snooping querier vlan 5
IP address           :5.5.5.10
IGMP version         :v3
Port                 :Fa3/1
Max response time    :10s
Query interval       :60s
Robustness variable  :2
Switch>
```

This example shows how to display snooping information for a specific group:

```
Switch# show ip igmp snooping group

Vlan      Group          Version  Ports
-----
2         224.0.1.40     v3       Router
2         224.2.2.2      v3       Fa6/2
Switch>
```

This example shows how to display the group's host types and ports in VLAN 1:

```
Switch# show ip igmp snooping group vlan 1
Vlan      Group          Host Type  Ports
-----
1         229.2.3.4      v3         fa2/1 fa2/3
1         224.2.2.2      v3         Fa6/2
Switch>
```

This example shows how to display the group's host types and ports in VLAN 1:

```
Switch# show ip igmp snooping group vlan 10 226.6.6.7
Vlan      Group          Version  Ports
-----
10        226.6.6.7      v3       Fa7/13, Fa7/14
Switch>
```

This example shows how to display the current state of a group with respect to a source IP address:

```
Switch# show ip igmp snooping group vlan 10 226.6.6.7 sources
Source information for group 226.6.6.7:
Timers: Expired sources are deleted on next IGMP General Query

SourceIP      Expires      Uptime      Inc Hosts  Exc Hosts
-----
2.0.0.1       00:03:04    00:03:48    2          0
2.0.0.2       00:03:04    00:02:07    2          0
Switch>
```

This example shows how to display the current state of a group with respect to a host MAC address:

```
Switch# show ip igmp snooping group vlan 10 226.6.6.7 hosts
IGMPv3 host information for group 226.6.6.7
Timers: Expired hosts are deleted on next IGMP General Query

Host (MAC/IP)  Filter mode    Expires    Uptime     # Sources
-----
175.1.0.29     INCLUDE      stopped   00:00:51   2
175.2.0.30     INCLUDE      stopped   00:04:14   2
Switch>
```

This example shows how to display summary information for a v3 group:

```
Switch# show ip igmp snooping group vlan 10 226.6.6.7 summary
Group Address (Vlan 10)      : 226.6.6.7
Host type                    : v3
Member Ports                 : Fa7/13, Fa7/14
Filter mode                  : INCLUDE
Expires                      : stopped
Sources                      : 2
Reporters (Include/Exclude) : 2/0
Switch>
```

This example shows how to display multicast router information for VLAN 1:

```
Switch# show ip igmp snooping mrouter vlan 1
vlan          ports
-----
1             Gi1/1,Gi2/1,Fa3/48,Router
Switch#
```

This example shows how to display the total number of group addresses learned by the system globally:

```
Switch# show ip igmp snooping group count
Total number of groups: 54
Switch>
```

This example shows how to display the total number of group addresses learned on VLAN 5:

```
Switch# show ip igmp snooping group vlan 5 count
Total number of groups: 30
Switch>
```

Related Commands

- [ip igmp snooping](#)
- [ip igmp snooping vlan immediate-leave](#)
- [ip igmp snooping vlan mrouter](#)
- [ip igmp snooping vlan static](#)
- [show ip igmp interface](#)
- [show ip igmp snooping mrouter](#)
- [show mac-address-table multicast](#)

show ip igmp snooping membership

To display host membership information, use the **show ip igmp snooping membership** command.

```
show ip igmp snooping membership [interface interface_num] [vlan vlan_id]
[reporter a.b.c.d] [source a.b.c.d group a.b.c.d]
```

Syntax Description	
interface <i>interface_num</i>	(Optional) Displays IP address and version information of an interface.
vlan <i>vlan_id</i>	(Optional) Displays VLAN members sorted by group IP address of a VLAN; valid values are from 1 to 1001 and from 1006 to 4094.
reporter <i>a.b.c.d</i>	(Optional) Displays membership information for a specified reporter.
source <i>a.b.c.d</i>	(Optional) Specifies a reporter, source, or group IP address.
group <i>a.b.c.d</i>	(Optional) Displays all members of a channel (source, group), sorted by interface or VLAN.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines This command is valid only if explicit host tracking is enabled on the switch.

Examples This example shows how to display host membership for interface gi4/1:

```
Switch# show ip igmp snooping membership interface gi4/1
#channels: 5
#hosts : 1
Source/Group Interface Reporter Uptime Last-Join Last-Leave

40.40.40.2/224.10.10.10 Gi4/1 20.20.20.20 00:23:37 00:06:50 00:20:30
40.40.40.4/224.10.10.10Gi4/1 20.20.20.20 00:39:42 00:09:17 -
Switch#
```

This example shows how to display host membership for VLAN 20 and group 224.10.10.10:

```
Switch# show ip igmp snooping membership vlan 20 source 40.40.40.2 group 224.10.10.10
#channels: 5
#hosts : 1
Source/Group Interface Reporter Uptime Last-Join Last-Leave

40.40.40.2/224.10.10.10 Gi4/1 20.20.20.20 00:23:37 00:06:50 00:20:30
Switch#
```


This example shows how to display host membership information for VLAN 20 and to delete the explicit host tracking:

```
Switch# show ip igmp snooping membership vlan 20
Snooping Membership Summary for Vlan 20
-----
Total number of channels:5
Total number of hosts   :4

Source/Group                Interface  Reporter      Uptime   Last-Join/
-----
40.0.0.1/224.1.1.1          Fa7/37    0002.4ba0.a4f6 00:00:04 00:00:04 /
-
40.0.0.2/224.1.1.1          Fa7/37    0002.fd80.f770 00:00:17 00:00:17 /
-
40.0.0.3/224.1.1.1          Fa7/36    20.20.20.20    00:00:04 00:00:04 /
-
40.0.0.4/224.1.1.1          Fa7/35    20.20.20.210   00:00:17 00:00:17 /
-
40.0.0.5/224.1.1.1          Fa7/37    0002.fd80.f770 00:00:17 00:00:17 /
-

Switch# clear ip igmp snooping membership vlan 20
Switch#
```

Related Commands

[clear ip igmp snooping membership](#)
[ip igmp snooping vlan explicit-tracking](#)
[show ip igmp snooping vlan](#)

show ip igmp snooping mrouter

To display information on dynamically learned and manually configured multicast switch interfaces, use the **show ip igmp snooping mrouter** command.

```
show ip igmp snooping mrouter [{vlan vlan-id}]
```

Syntax Description	vlan <i>vlan-id</i> (Optional) Specifies a VLAN; valid values are from 1 to 1001 and from 1006 to 4094.
---------------------------	--

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(19)EW	Added support for extended VLAN addresses.

Usage Guidelines	<p>You can also use the show mac-address-table multicast command to display entries in the MAC address table for a VLAN that has IGMP snooping enabled.</p> <p>You can display IGMP snooping information for VLAN interfaces by entering the show ip igmp interface vlan <i>vlan-num</i> command.</p>
-------------------------	--

Examples	This example shows how to display snooping information for a specific VLAN:
-----------------	---

```
Switch# show ip igmp snooping mrouter vlan 1
vlan                ports
-----+-----
 1                Gi1/1,Gi2/1,Fa3/48,Switch
Switch#
```

Related Commands	ip igmp snooping vlan mrouter show ip igmp interface show mac-address-table multicast
-------------------------	---

show ip igmp snooping vlan

To display information on dynamically learned and manually configured VLAN switch interfaces, use the **show ip igmp snooping vlan** command.

show ip igmp snooping vlan *vlan_num*

Syntax Description	<i>vlan_num</i> Number of the VLAN; valid values are from 1 to 1001 and from 1006 to 4094.
---------------------------	--

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Support for extended addressing was added.	

Usage Guidelines	You can also use the show mac-address-table multicast command to display entries in the MAC address table for a VLAN that has IGMP snooping enabled.
-------------------------	---

Examples	This example shows how to display snooping information for a specific VLAN:
-----------------	---

```
Switch# show ip igmp snooping vlan 2
vlan 2
-----
IGMP snooping is globally enabled
IGMP snooping TCN solicit query is globally enabled
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 is running in IGMP_ONLY mode on this Vlan
Switch#
```

Related Commands	ip igmp snooping ip igmp snooping vlan immediate-leave ip igmp snooping vlan mrouter ip igmp snooping vlan static show ip igmp interface show ip igmp snooping mrouter show mac-address-table multicast
-------------------------	---

show ip mfib

To display all active Multicast Forwarding Information Base (MFIB) routes, use the **show ip mfib** command.

```
show ip mfib [all | counters | log [n]]
```

Syntax Description	all	(Optional) Specifies all routes in the MFIB, including those routes that are used to accelerate fast switching but that are not necessarily in the upper-layer routing protocol table.
	counters	(Optional) Specifies the counts of MFIB-related events. Only non-zero counters are shown.
	log	(Optional) Specifies a log of the most recent number of MFIB-related events. The most recent event is first.
	<i>n</i>	(Optional) Specifies the number of events.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines The MFIB table contains a set of IP multicast routes; each route in the MFIB table contains several flags that associate to the route.

The route flags indicate how a packet that matches a route is forwarded. For example, the IC flag on an MFIB route indicates that some process on the switch needs to receive a copy of the packet. The following flags are associated with MFIB routes:

- Internal Copy (IC) flag—Set on a route when a process on the switch needs to receive a copy of all packets matching the specified route.
- Signaling (S) flag—Set on a route when a switch process needs notification that a packet matching the route is received. In the expected behavior, the protocol code updates the MFIB state in response to having received a packet on a signaling interface.
- Connected (C) flag—When set on a route, the C flag has the same meaning as the S flag, except that the C flag indicates that only packets sent by directly connected hosts to the route should be signaled to a protocol process.

A route can also have a set of flags associated with one or more interfaces. For an (S,G) route, the flags on interface 1 indicate how ingress packets should be treated and whether packets matching the route should be forwarded onto interface 1. The following per-interface flags are associated with MFIB routes:

- Accepting (A)—Set on the RPF interface when a packet that arrives on the interface and that is marked as Accepting (A) is forwarded to all Forwarding (F) interfaces.

- Forwarding (F)—Used in conjunction with the A flag as described above. The set of forwarding interfaces together form a multicast list or output interface list.
- Signaling (S)—Set on an interface when a multicast routing protocol process in Cisco IOS needs to be notified of ingress packets on that interface.
- Not Platform (NP) fast-switched—Used in conjunction with the F flag. A forwarding interface is also marked as Not Platform fast-switched whenever that output interface cannot be fast-switched by the platform hardware and requires software forwarding.

For example, the Catalyst 4006 switch with Supervisor EngineIII cannot switch tunnel interfaces in hardware so these interfaces are marked with the NP flag. When an NP interface is associated with a route, a copy of every ingress packet arriving on an Accepting interface is sent to the switch software forwarding path for software replication and then forwarded to the NP interface.

Examples

This example shows how to display all active MFIB routes:

```
Switch# show ip mfib
IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal,
             IC - Internal Copy
Interface Flags: A - Accept, F - Forward, NS - Signal,
                NP - Not platform switched
Packets: Fast/Partial/Slow Bytes: Fast/Partial/Slow:
(171.69.10.13, 224.0.1.40), flags (IC)
  Packets: 2292/2292/0, Bytes: 518803/0/518803
  Vlan7 (A)
  Vlan100 (F NS)
  Vlan105 (F NS)
(*, 224.0.1.60), flags ()
  Packets: 2292/0/0, Bytes: 518803/0/0
  Vlan7 (A NS)
(*, 224.0.1.75), flags ()
  Vlan7 (A NS)
(10.34.2.92, 239.192.128.80), flags ()
  Packets: 24579/100/0, 2113788/15000/0 bytes
  Vlan7 (F NS)
  Vlan100 (A)
(*, 239.193.100.70), flags ()
  Packets: 1/0/0, 1500/0/0 bytes
  Vlan7 (A)
Switch#
```

Related Commands [clear ip mfib counters](#)

show ip mfib fastdrop

To show all currently active fast drop entries and to show whether fast drop is enabled, use the **show ip mfib fastdrop** command.

show ip mfib fastdrop

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to display all currently active fast drop entries and whether fast drop is enabled.

```
Switch# show ip mfib fastdrop
MFIB fastdrop is enabled.
MFIB fast-dropped flows:
(10.0.0.1, 224.1.2.3, Vlan9 ) 00:01:32
(10.1.0.2, 224.1.2.3, Vlan9 ) 00:02:30
(1.2.3.4, 225.6.7.8, Vlan3) 00:01:50
Switch#
```

Related Commands [clear ip mfib fastdrop](#)

show ip mroute

To display IP multicast routing table information, use the **show ip mroute** command.

```
show ip mroute [interface_type slot/port | host_name | host_address [source] | active [kbps | interface_type num] | count | pruned | static | summary]
```

Syntax Description	
<i>interface_type slot/port</i>	(Optional) Interface type and number of the slot and port; valid values for <i>interface type</i> are FastEthernet , GigabitEthernet , null , and vlan .
<i>host_name</i>	(Optional) Name or IP address as defined in the DNS hosts table.
<i>host_address source</i>	(Optional) IP address or name of a multicast source.
active	(Optional) Displays the rate that active sources are sending to multicast groups.
<i>kbps interface_type num</i>	(Optional) Minimum rate at which active sources are sending to multicast groups; active sources sending at this rate or greater will be displayed. Valid values are from 1 to 4294967295 kbps.
count	(Optional) Displays route and packet count information.
pruned	(Optional) Displays pruned routes.
static	(Optional) Displays static multicast routes.
summary	(Optional) Displays a one-line, abbreviated summary of each entry in the IP multicast routing table.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

If you omit all optional arguments and keywords, the **show ip mroute** command displays all entries in the IP multicast routing table.

The **show ip mroute active kbps** command displays all sources sending at a rate greater than or equal to *kbps*.

The multicast routing table is populated by creating source, group (S,G) entries from star, group (*,G) entries. The star refers to all source addresses, the “S” refers to a single source address, and the “G” is the destination multicast group address. In creating (S,G) entries, the software uses the best path to that destination group found in the unicast routing table (that is, through Reverse Path Forwarding (RPF)).

Examples

This example shows how to display all entries in the IP multicast routing table:

```
Switch# show ip mroute

IP Multicast Routing Table
Flags:D - Dense, S - Sparse, s - SSM Group, C - Connected, L - Local,
      P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
      J - Join SPT, M - MSDP created entry, X - Proxy Join Timer Running
      A - Advertised via MSDP, U - URD, I - Received Source Specific Host
      Report
Outgoing interface flags:H - Hardware switched
Timers:Uptime/Expires
Interface state:Interface, Next-Hop or VCD, State/Mode

(*, 230.13.13.1), 00:16:41/00:00:00, RP 10.15.1.20, flags:SJC
  Incoming interface:GigabitEthernet4/8, RPF nbr 10.15.1.20
  Outgoing interface list:

GigabitEthernet4/9, Forward/Sparse-Dense, 00:16:41/00:00:00, H

(*, 230.13.13.2), 00:16:41/00:00:00, RP 10.15.1.20, flags:SJC

  Incoming interface:GigabitEthernet4/8, RPF nbr 10.15.1.20, RPF-MFD
  Outgoing interface list:
    GigabitEthernet4/9, Forward/Sparse-Dense, 00:16:41/00:00:00, H

(10.20.1.15, 230.13.13.1), 00:14:31/00:01:40, flags:CJT

  Incoming interface:GigabitEthernet4/8, RPF nbr 10.15.1.20, RPF-MFD
  Outgoing interface list:
    GigabitEthernet4/9, Forward/Sparse-Dense, 00:14:31/00:00:00, H

(132.206.72.28, 224.2.136.89), 00:14:31/00:01:40, flags:CJT
  Incoming interface:GigabitEthernet4/8, RPF nbr 10.15.1.20, RPF-MFD

  Outgoing interface list:Null
Switch#
```

This example shows how to display the rate that active sources are sending to multicast groups and to display only active sources sending at greater than the default rate:

```
Switch# show ip mroute active

Active IP Multicast Sources - sending > = 4 kbps

Group: 224.2.127.254, (sdr.cisco.com)
  Source: 146.137.28.69 (mbone.ipd.anl.gov)
  Rate: 1 pps/4 kbps(1sec), 4 kbps(last 1 secs), 4 kbps(life avg)

Group: 224.2.201.241, ACM 97
  Source: 130.129.52.160 (webcast3-e1.acm97.interop.net)
  Rate: 9 pps/93 kbps(1sec), 145 kbps(last 20 secs), 85 kbps(life avg)

Group: 224.2.207.215, ACM 97
  Source: 130.129.52.160 (webcast3-e1.acm97.interop.net)
  Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
Switch#
```

This example shows how to display route and packet count information:

```
Switch# show ip mroute count

IP Multicast Statistics
56 routes using 28552 bytes of memory
13 groups, 3.30 average sources per group
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
```



```

Other counts:Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group:224.2.136.89, Source count:1, Group pkt count:29051
  Source:132.206.72.28/32, Forwarding:29051/-278/1186/0, Other:85724/8/56665
Switch#

```

This example shows how to display summary information:

```

Switch# show ip mroute summary
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, s - SSM Group, C - Connected, L - Local,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT, M - MSDP created entry, X - Proxy Join Timer Running
       A - Advertised via MSDP, U - URD, I - Received Source Specific Host
       Report
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

Switch#

```

Table2-16 describes the fields shown in the output.

Table2-16 show ip mroute Field Descriptions

Field	Description
Flags:	Information about the entry.
D - Dense	Entry is operating in dense mode.
S - Sparse	Entry is operating in sparse mode.
s - SSM Group	Entry is a member of an SSM group.
C - Connected	Member of the multicast group is present on the directly connected interface.
L - Local	Switch itself is a member of the multicast group.
P - Pruned	Route has been pruned. This information is retained in case a downstream member wants to join the source.
R - Rp-bit set	Status of the (S,G) entry; is the (S,G) entry pointing toward the RP. The R - Rp-bit set is typically a prune state along the shared tree for a particular source.
F - Register flag	Status of the software; is the software registered for a multicast source.
T - SPT-bit set	Status of the packets; have the packets been received on the shortest path source tree.

Table2-16 show ip mroute Field Descriptions (continued)

Field	Description
J - Join SPT	<p>For (*, G) entries, indicates that the rate of traffic flowing down the shared tree is exceeding the SPT-Threshold set for the group. (The default SPT-Threshold setting is 0kbps.) When the J - Join SPT flag is set, the next (S,G) packet received down the shared tree triggers an (S,G) join in the direction of the source causing the switch to join the source tree.</p> <p>For (S, G) entries, indicates that the entry was created because the SPT-Threshold for the group was exceeded. When the J - Join SPT flag is set for (S,G) entries, the switch monitors the traffic rate on the source tree and attempts to switch back to the shared tree for this source if the traffic rate on the source tree falls below the group's SPT-Threshold for more than one minute.</p> <p>The switch measures the traffic rate on the shared tree and compares the measured rate to the group's SPT-Threshold once every second. If the traffic rate exceeds the SPT-Threshold, the J-Join SPT flag is set on the (*, G) entry until the next measurement of the traffic rate. The flag is cleared when the next packet arrives on the shared tree and a new measurement interval is started.</p> <p>If the default SPT-Threshold value of 0 Kbps is used for the group, the J- Join SPT flag is always set on (*, G) entries and is never cleared. When the default SPT-Threshold value is used, the switch immediately switches to the shortest-path tree when traffic from a new source is received.</p>
Outgoing interface flag:	Information about the outgoing entry.
H - Hardware switched	Entry is hardware switched.
Timer:	Uptime/Expires.
Interface state:	Interface, Next-Hop or VCD, State/Mode.
(*, 224.0.255.1) (198.92.37.100/32, 224.0.255.1)	<p>Entry in the IP multicast routing table. The entry consists of the IP address of the source switch followed by the IP address of the multicast group. An asterisk (*) in place of the source switch indicates all sources.</p> <p>Entries in the first format are referred to as (*,G) or "star comma G" entries. Entries in the second format are referred to as (S,G) or "S commaG" entries. (*,G) entries are used to build (S,G) entries.</p>
uptime	How long (in hours, minutes, and seconds) the entry has been in the IP multicast routing table.
expires	How long (in hours, minutes, and seconds) until the entry is removed from the IP multicast routing table on the outgoing interface.

Table2-16 show ip mroute Field Descriptions (continued)

Field	Description
RP	Address of the RP switch. For switches and access servers operating in sparse mode, this address is always 0.0.0.0.
flags:	Information about the entry.
Incoming interface	Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.
RPF neighbor	IP address of the upstream switch to the source. "Tunneling" indicates that this switch is sending data to the RP encapsulated in Register packets. The hexadecimal number in parentheses indicates to which RP it is registering. Each bit indicates a different RP if multiple RPs per group are used.
DVMRP or Mroute	Status of whether the RPF information is obtained from the DVMRP routing table or the static mroutes configuration.
Outgoing interface list	Interfaces through which packets are forwarded. When the ip pim nbma-mode command is enabled on the interface, the IP address of the PIM neighbor is also displayed.
Ethernet0	Name and number of the outgoing interface.
Next hop or VCD	Next hop specifies downstream neighbor's IP address. VCD specifies the virtual circuit descriptor number. VCD0 means the group is using the static-map virtual circuit.
Forward/Dense	Status of the packets; are they forwarded on the interface if there are no restrictions due to access lists or the TTL threshold. Following the slash (/), mode in which the interface is operating (dense or sparse).
Forward/Sparse	Sparse mode interface is in forward mode.
time/time (uptime/expiration time)	Per interface, how long (in hours, minutes, and seconds) the entry has been in the IP multicast routing table. Following the slash (/), how long (in hours, minutes, and seconds) until the entry is removed from the IP multicast routing table.

Related Commands**ip multicast-routing** (refer to Cisco IOS documentation)**ip pim** (refer to Cisco IOS documentation)

show ip source binding

To display IP source bindings configured on the system, use the **show ip source binding EXEC** command.

```
show ip source binding [ip-address] [mac-address] [dhcp-snooping | static] [vlan vlan-id]
[interface interface-name]
```

Syntax Description	
<i>ip-address</i>	(Optional) Binding IP address.
<i>mac-address</i>	(Optional) Binding MAC address.
dhcp-snooping	(Optional) DHCP-snooping type binding.
static	(Optional) Statically configured binding.
vlan <i>vlan-id</i>	(Optional) VLAN number.
interface <i>interface-name</i>	(Optional) Binding interface.

Defaults Displays both static and DHCP snooping bindings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(19)EW	This command was first introduced.

Usage Guidelines The optional parameters filter the display output result.

Examples This example shows how to display the IP source bindings:

```
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    FastEthernet6/10

Switch#
```

This example shows how to display the static IP binding entry of IP address 11.0.0.1:

```
Switch# show ip source binding 11.0.0.1 0000.000A.000B static vlan 10 interface Fa6/10
show ip source binding 11.0.0.1 0000.000A.000B static vlan 10 interface Fa6/10
MacAddress      IpAddress      Lease(sec)  Type           VLAN  Interface
-----
00:00:00:0A:00:0B  11.0.0.1      infinite    static         10    FastEthernet6/10

Switch#
```

Related Commands [ip source binding](#)

show ip verify source

To display IP source guard configuration and filters on a particular interface, use the **show ip verify source** command.

show ip verify source [**interface** *interface_num*]

Syntax Description	interface <i>interface_num</i> (Optional) Specifies an interface.				
Defaults	This command has no default settings.				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(19)EW</td> <td>Support for this command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Release	Modification				
12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.				

Examples

These examples show how to display IP source guard configuration and filters on a particular interface with the **show ip verify source interface** command:

- The following output appears when DHCP snooping is enabled on VLAN 10-20, interface fa6/1 has IP source filter mode configured as IP, and an existing IP address binding 10.0.0.1 is on VLAN 10:

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
fa6/1	ip	active	10.0.0.1		10
fa6/1	ip	active	deny-all		11-20



Note The second entry shows that a default PVACL (deny all IP traffic) is installed on the port for those snooping-enabled VLANs that do not have a valid IP source binding.

- The following output appears when you enter the **show ip verify source interface fa6/2** command and DHCP snooping is enabled on VLAN 10-20, interface fa6/1 has IP source filter mode configured as IP, and there is an existing IP address binding 10.0.0.1 on VLAN 10:

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
fa6/2	ip	inactive-trust-port			

- The following output appears when you enter the **show ip verify source interface fa6/3** command and the interface fa6/3 does not have a VLAN enabled for DHCP snooping:

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
fa6/3	ip	inactive-no-snooping-vlan			

show ip verify source

- The following output appears when you enter the **show ip verify source interface fa6/4** command and the interface fa6/4 has IP source filter mode configured as IP MAC, and existing IP MAC that binds 10.0.0.2/aaaa.bbbb.cccc on VLAN 10 and 11.0.0.1/aaaa.bbbb.cccd on VLAN 11 :

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
fa6/4	ip-mac	active	10.0.0.2	aaaa.bbbb.cccc	10
fa6/4	ip-mac	active	11.0.0.1	aaaa.bbbb.cccd	11
fa6/4	ip-mac	active	deny-all	deny-all	12-20

- The following output appears when you enter the **show ip verify source interface fa6/5** command and the interface fa6/5 has IP source filter mode configured as IP MAC, and existing IP MAC binding 10.0.0.3/aaaa.bbbb.cccc on vlan 10, but port security is not enabled on fa6/5:

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
fa6/5	ip-mac	active	10.0.0.3	permit-all	10
fa6/5	ip-mac	active	deny-all	permit-all	11-20



Note Enable port security first because the DHCP security MAC filter cannot apply to the port or VLAN.

- The following output appears when you enter the **show ip verify source interface fa6/6** command and the interface fa6/6 does not have IP source filter mode configured:

```
DHCP security is not configured on the interface fa6/6.
```

This example shows how to display all interfaces on the switch that have DHCP snooping security enabled with the **show ip verify source** command.

The output is an accumulation of per-interface **show** CLIs:

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
fa6/1	ip	active	10.0.0.1		10
fa6/1	ip	active	deny-all		11-20
fa6/2	ip	inactive-trust-port			
fa6/3	ip	inactive-no-snooping-vlan			
fa6/4	ip-mac	active	10.0.0.2	aaaa.bbbb.cccc	10
fa6/4	ip-mac	active	11.0.0.1	aaaa.bbbb.cccd	11
fa6/4	ip-mac	active	deny-all	deny-all	12-20
fa6/5	ip-mac	active	10.0.0.3	permit-all	10
fa6/5	ip-mac	active	deny-all	permit-all	11-20

Related Commands

[ip igmp snooping](#)
[ip dhcp snooping information option](#)
[ip dhcp snooping limit rate](#)
[ip dhcp snooping trust](#)
[ip igmp snooping vlan](#)
[ip source binding](#)
[ip verify source vlan dhcp-snooping](#)
[show ip source binding](#)

show ipc

To display IPC information, use the **show ipc** command.

show ipc { nodes | ports | queue | status }

Syntax Description	nodes	Displays participating nodes.
	ports	Displays local IPC ports.
	queue	Displays the contents of the IPC retransmission queue.
	status	Displays the status of the local IPC server.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to display participating nodes:

```
Switch# show ipc nodes
There are 3 nodes in this IPC realm.
  ID      Type      Name                               Last Sent  Last Heard
  10000   Local      IPC Master                         0          0
  2010000 Local      GALIOS IPC:Card 1                  0          0
  2020000 Ethernet  GALIOS IPC:Card 2                  12         26
Switch#
```

This example shows how to display local IPC ports:

```
Switch# show ipc ports
There are 11 ports defined.
Port ID      Type      Name                               (current/peak/total)
  10000.1     unicast  IPC Master:Zone
  10000.2     unicast  IPC Master:Echo
  10000.3     unicast  IPC Master:Control
  10000.4     unicast  Remote TTY Server Port
  10000.5     unicast  GALIOS RF :Active
    index = 0 seat_id = 0x2020000 last sent = 0 heard = 1635 0/1/1635
  10000.6     unicast  GALIOS RED:Active
    index = 0 seat_id = 0x2020000 last sent = 0 heard = 2 0/1/2
  2020000.3   unicast  GALIOS IPC:Card 2:Control
  2020000.4   unicast  GALIOS RFS :Standby
  2020000.5   unicast  Slave: Remote TTY Client Port
  2020000.6   unicast  GALIOS RF :Standby
  2020000.7   unicast  GALIOS RED:Standby
```

```
RPC packets: current/peak/total
```

```
0/1/17
```

```
Switch#
```

This example shows how to display the contents of the IPC retransmission queue:

```
Switch# show ipc queue
```

```
There are 0 IPC messages waiting for acknowledgement in the transmit queue.
```

```
There are 0 IPC messages waiting for a response.
```

```
There are 0 IPC messages waiting for additional fragments.
```

```
There are 0 IPC messages currently on the IPC inboundQ.
```

```
There are 0 messages currently in use by the system.
```

```
Switch#
```

This example shows how to display the status of the local IPC server:

```
Switch# show ipc status
```

```
IPC System Status:
```

```
This processor is the IPC master server.
```

```
6000 IPC message headers in cache
```

```
3363 messages in, 1680 out, 1660 delivered to local port,
```

```
1686 acknowledgements received, 1675 sent,
```

```
0 NACKS received, 0 sent,
```

```
0 messages dropped on input, 0 messages dropped on output
```

```
0 no local port, 0 destination unknown, 0 no transport
```

```
0 missing callback or queue, 0 duplicate ACKs, 0 retries,
```

```
0 message timeouts.
```

```
0 ipc_output failures, 0 mtu failures,
```

```
0 msg alloc failed, 0 emer msg alloc failed, 0 no origs for RPC replies
```

```
0 pak alloc failed, 0 memd alloc failed
```

```
0 no hwq, 1 failed opens, 0 hardware errors
```

```
No regular dropping of IPC output packets for test purposes
```

```
Switch#
```


show l2protocol-tunnel

To display information about Layer 2 protocol tunnel ports, use the **show l2protocol-tunnel** command. This command displays information for interfaces with protocol tunneling enabled.

```
show l2protocol-tunnel [interface interface-id] [summary] | { begin | exclude | include }
expression ]
```

Syntax Description	
interface <i>interface-id</i>	(Optional) Specifies the interface for which protocol tunneling information appears. Valid interfaces are physical ports and port channels; the port channel range is 1 to 64.
summary	(Optional) Displays only Layer 2 protocol summary information.
begin	(Optional) Displays information beginning with the line that matches the <i>expression</i> .
exclude	(Optional) Displays information that excludes lines that match the <i>expression</i> .
include	(Optional) Displays lines that match the specified <i>expression</i> .
<i>expression</i>	(Optional) Expression in the output to use as a reference point.

Command Modes	
	User EXEC

Command History	Release	Modification
	12.2(18)EW	This command was first introduced on the Catalyst 4500 series switch.

Usage Guidelines After enabling Layer 2 protocol tunneling on an access or 802.1Q tunnel port with the **l2protocol-tunnel** command, you can configure some or all of these parameters:

- Protocol type to be tunneled
- Shutdown threshold
- Drop threshold

If you enter the **show l2protocol-tunnel [interface interface-id]** command, only information about the active ports on which all the parameters are configured appears.

If you enter the **show l2protocol-tunnel summary** command, only information about the active ports on which some or all of the parameters are configured appears.

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

```
show l2protocol-tunnel
```

Examples

This is an example of output from the **show l2protocol-tunnel** command:

```
Switch> show l2protocol-tunnel
COS for Encapsulated Packets: 5
```

Port	Protocol	Shutdown Threshold	Drop Threshold	Encapsulation Counter	Decapsulation Counter	Drop Counter
Fa0/10	stp	----	----	9847	1866	0
	vtp	----	----	77	12	0
	pagp	----	----	859	860	0
	lacp	----	----	0	0	0
	udld	----	----	219	211	0
Fa0/11	cdp	1100	----	2356	2350	0
	stp	1100	----	116	13	0
	vtp	1100	----	3	67	0
	pagp	----	900	856	5848	0
	lacp	----	900	0	0	0
Fa0/12	udld	----	900	0	0	0
	cdp	----	----	2356	0	0
	stp	----	----	11787	0	0
	vtp	----	----	81	0	0
	pagp	----	----	0	0	0
Fa0/13	lacp	----	----	849	0	0
	udld	----	----	0	0	0
	cdp	----	----	2356	0	0
	stp	----	----	11788	0	0
	vtp	----	----	81	0	0
Fa0/14	pagp	----	----	0	0	0
	lacp	----	----	849	0	0
	udld	----	----	0	0	0
	cdp	----	----	2356	0	0
	stp	----	----	11788	0	0

This is an example of output from the **show l2protocol-tunnel summary** command:

```
Switch> show l2protocol-tunnel summary
COS for Encapsulated Packets: 5
```

Port	Protocol	Shutdown Threshold (cdp/stp/vtp) (pagp/lacp/udld)	Drop Threshold (cdp/stp/vtp) (pagp/lacp/udld)	Status
Fa0/10	stp vtp	----/----/----	----/----/----	up
	pagp lacp udld	----/----/----	----/----/----	
Fa0/11	cdp stp vtp	1100/1100/1100	----/----/----	up
	pagp lacp udld	----/----/----	900/ 900/ 900	
Fa0/12	cdp stp vtp	----/----/----	----/----/----	up
	pagp lacp udld	----/----/----	----/----/----	
Fa0/13	cdp stp vtp	----/----/----	----/----/----	up
	pagp lacp udld	----/----/----	----/----/----	
Fa0/14	cdp stp vtp	----/----/----	----/----/----	down
	pagp ---- udld	----/----/----	----/----/----	
Fa0/15	cdp stp vtp	----/----/----	----/----/----	down
	pagp ---- udld	----/----/----	----/----/----	
Fa0/16	cdp stp vtp	----/----/----	----/----/----	down
	pagp lacp udld	----/----/----	----/----/----	
Fa0/17	cdp stp vtp	----/----/----	----/----/----	down
	pagp lacp udld	----/----/----	----/----/----	

Related Commands **clear l2protocol-tunnel counter** (refer to Cisco IOS documentation)
[l2protocol-tunnel](#)
[l2protocol-tunnel cos](#)

show lacp

To display LACP information, use the **show lacp** command.

```
show lacp [channel-group] { counters | internal | neighbors | sys-id }
```

Syntax Description	
<i>channel-group</i>	(Optional) Number of the channel group; valid values are from 1 to 64.
counters	Displays the LACP statistical information.
internal	Displays the internal information.
neighbors	Displays the neighbor information.
sys-id	Displays the LACP system identification.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst4500 series switches.

Usage Guidelines This command is not supported on systems configured with a Supervisor Engine 1.

If you do not specify a *channel-group* value, all channel groups are displayed.

You can enter the optional *channel-group* value, to specify a channel group for all keywords, except the **sys-id** keyword.

Examples This example shows how to display LACP statistical information for a specific channel group:

```
Switch# show lacp 1 counters
          LACPDU          Marker          LACPDU
Port      Sent  Recv      Sent  Recv      Pkts  Err
-----
Channel group: 1
  Fa4/1    8    15         0    0         3    0
  Fa4/2   14   18         0    0         3    0
  Fa4/3   14   18         0    0         0
  Fa4/4   13   18         0    0         0
Switch#
```

The output displays the following information:

- The LACPDU Sent and Recv columns display the LACPDU sent and received on each specific interface.
- The LACPDU Pkts and Err columns display the marker protocol packets.

This example shows how to display internal information for the interfaces belonging to a specific channel:

```
Switch# show lacp 1 internal
Flags: S - Device sends PDUs at slow rate. F - Device sends PDUs at fast rate.
      A - Device is in Active mode.           P - Device is in Passive mode.

Channel group 1

Port      Flags   State   LACPDU  LACP Port  Admin  Oper   Port   Port
Port      Flags   State   Interval Priority    Key    Key    Number State
Fa4/1     saC     bndl    30s     32768      100   100   0xc1  0x75
Fa4/2     saC     bndl    30s     32768      100   100   0xc2  0x75
Fa4/3     saC     bndl    30s     32768      100   100   0xc3  0x75
Fa4/4     saC     bndl    30s     32768      100   100   0xc4  0x75
Switch#
```

Table2-17 lists the output field definitions.

Table2-17 show lacp internal Command Output Fields

Field	Description
State	State of the specific port at the current moment is displayed; allowed values are as follows: <ul style="list-style-type: none"> <i>bndl</i>—Port is attached to an aggregator and bundled with other ports. <i>susp</i>—Port is in a suspended state; it is not attached to any aggregator. <i>indep</i>—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). <i>hot-sby</i>—Port is in a Hot-standby state. <i>down</i>—Port is down.
LACPDU Interval	Interval setting.
LACP Port Priority	Port priority setting.
Admin Key	Administrative key.
Oper Key	Operator key.
Port Number	Port number.
Port State	State variables for the port encoded as individual bits within a single octet with the following meaning [1]: <ul style="list-style-type: none"> bit0: <i>LACP_Activity</i> bit1: <i>LACP_Timeout</i> bit2: <i>Aggregation</i> bit3: <i>Synchronization</i> bit4: <i>Collecting</i> bit5: <i>Distributing</i> bit6: <i>Defaulted</i> bit7: <i>Expired</i>

This example shows how to display LACP neighbors information for a specific port channel:

```
Switch# show lacp 1 neighbor
Flags: S - Device sends PDUs at slow rate. F - Device sends PDUs at fast rate.
       A - Device is in Active mode.           P - Device is in Passive mode.

Channel group 1 neighbors

      Partner
Port   System ID          Partner      Age   Flags
Fa4/1  8000,00b0.c23e.d84e   0x81        29s   P
Fa4/2  8000,00b0.c23e.d84e   0x82         0s   P
Fa4/3  8000,00b0.c23e.d84e   0x83         0s   P
Fa4/4  8000,00b0.c23e.d84e   0x84         0s   P

      Port      Admin   Oper   Port
      Priority  Key     Key     State
Fa4/1  32768    200    200    0x81
Fa4/2  32768    200    200    0x81
Fa4/3  32768    200    200    0x81
Fa4/4  32768    200    200    0x81
Switch#
```

In the case where no PDUs have been received, the default administrative information is displayed in braces.

This example shows how to display the LACP system identification:

```
Switch> show lacp sys-id
8000,AC-12-34-56-78-90
Switch>
```

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

[lacp port-priority](#)
[lacp system-priority](#)

show mac access-group interface

To display the ACL configuration on a Layer 2 interface, use the **show mac access-group interface** command.

show mac access-group interface [*interface interface-number*]

Syntax Description	<i>interface</i>	(Optional) Specifies the interface type. Valid values are ethernet , fastethernet , gigabitethernet , tengigabitethernet , pos , atm , port-channel , and ge-wan .
	<i>interface-number</i>	(Optional) Specifies the port number.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Valid values for the port number depend on the chassis used.

Examples This example shows how to display the ACL configuration on interface fast 6/1:

```
Switch# show mac access-group interface fast 6/1
Interface FastEthernet6/1:
  Inbound access-list is simple-mac-acl
  Outbound access-list is not set
```

Related Commands [access-group mode](#)

show mac-address-table address

To display MAC address table information for a specific MAC address, use the **show mac-address-table address** command.

```
show mac-address-table address mac_addr [interface type slot/port | protocol protocol | vlan
vlan_id]
```

Syntax Description	
<i>mac_addr</i>	48-bit MAC address; the valid format is H.H.H.
interface <i>type slot/port</i>	(Optional) Displays information for a specific interface; valid values for <i>type</i> are FastEthernet and GigabitEthernet .
protocol <i>protocol</i>	(Optional) Specifies a protocol. See “Usage Guidelines” for more information.
vlan <i>vlan_id</i>	(Optional) Displays entries for the specific VLAN only; valid values are from 1 to 4094.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Added support for extended VLAN addresses.

Usage Guidelines For MAC address table entries used by routed ports, the routed port name is displayed in the “vlan” column rather than the internal VLAN number.

The keyword definitions for the *protocol* variable are as follows:

- **ip** specifies IP protocol.
- **ipx** specifies IPX protocols.
- **assigned** specifies assigned protocol entries.
- **other** specifies other protocol entries.

Examples This example shows how to display MAC address table information for a specific MAC address:

```
Switch# show mac-address-table address 0030.94fc.0dff
Unicast Entries
  vlan  mac address      type      protocols      port
-----+-----+-----+-----+-----
    1   0030.94fc.0dff    static   ip,ipx,assigned,other  Switch
Fa6/1   0030.94fc.0dff    static   ip,ipx,assigned,other  Switch
Fa6/2   0030.94fc.0dff    static   ip,ipx,assigned,other  Switch
Switch#
```

Related Commands

show mac-address-table aging-time
show mac-address-table count
show mac-address-table dynamic
show mac-address-table interface
show mac-address-table multicast
show mac-address-table protocol
show mac-address-table static
show mac-address-table vlan

show mac-address-table aging-time

To display the MAC address aging time, use the **show mac-address-table aging-time** command.

```
show mac-address-table aging-time [vlan vlan_id]
```

Syntax Description	vlan <i>vlan_id</i> (Optional) Specifies a VLAN; valid values are from 1 to 4094.
---------------------------	--

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended addressing was added.

Examples	This example shows how to display the currently configured aging time for all VLANs:
-----------------	--

```
Switch# show mac-address-table aging-time
Vlan    Aging Time
----    -
100     300
200     1000

Switch#
```

This example shows how to display the currently configured aging time for a specific VLAN:

```
Switch# show mac-address-table aging-time vlan 100
Vlan    Aging Time
----    -
100     300

Switch#
```

Related Commands	show mac-address-table address show mac-address-table count show mac-address-table dynamic show mac-address-table interface show mac-address-table multicast show mac-address-table protocol show mac-address-table static show mac-address-table vlan
-------------------------	---

show mac-address-table count

To display the number of entries currently in the MAC address table, use the **show mac-address-table count** command.

show mac-address-table count [**vlan** *vlan_id*]

Syntax Description	vlan <i>vlan_id</i> (Optional) Specifies a VLAN; valid values are from 1 to 4094.						
Defaults	This command has no default settings.						
Command Modes	Privileged EXEC						
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(8a)EW</td> <td>Support for this command was introduced on the Catalyst 4500 series switch.</td> </tr> <tr> <td>12.1(12c)EW</td> <td>Added support for extended VLAN addresses.</td> </tr> </tbody> </table>	Release	Modification	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.	12.1(12c)EW	Added support for extended VLAN addresses.
Release	Modification						
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.						
12.1(12c)EW	Added support for extended VLAN addresses.						

Examples This example shows how to display the entry count for a specific VLAN:

```
Switch# show mac-address-table count vlan 1
MAC Entries for Vlan 1:
Dynamic Unicast Address Count:          0
Static Unicast Address (User-defined) Count:  0
Static Unicast Address (System-defined) Count: 1
Total Unicast MAC Addresses In Use:          1
Total Unicast MAC Addresses Available:       32768
Multicast MAC Address Count:              1
Total Multicast MAC Addresses Available:     16384
Switch#
```

Related Commands

- [show mac-address-table address](#)
- [show mac-address-table aging-time](#)
- [show mac-address-table dynamic](#)
- [show mac-address-table interface](#)
- [show mac-address-table multicast](#)
- [show mac-address-table protocol](#)
- [show mac-address-table static](#)
- [show mac-address-table vlan](#)

show mac-address-table dynamic

To display dynamic MAC address table entries only, use the **show mac-address-table dynamic** command.

```
show mac-address-table dynamic [address mac_addr | interface type slot/port |
                                protocol protocol | vlan vlan_id]
```

Syntax Description	Parameter	Description
	address <i>mac_addr</i>	(Optional) Specifies a 48-bit MAC address; the valid format is H.H.H.
	interface <i>type slot/port</i>	(Optional) Specifies an interface to match; valid values for <i>type</i> are FastEthernet and GigabitEthernet .
	protocol <i>protocol</i>	(Optional) Specifies a protocol. See “Usage Guidelines” for more information.
	vlan <i>vlan_id</i>	(Optional) Displays entries for a specific VLAN; valid values are from 1 to 4094.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Added support for extended VLAN addresses.

Usage Guidelines The keyword definitions for the *protocol* argument are as follows:

- **assigned** specifies assigned protocol entries.
- **ip** specifies IP protocol.
- **ipx** specifies IPX protocols.
- **other** specifies other protocol entries.

The **show mac-address-table dynamic** command output for an EtherChannel interface changes the port number designation (for example, 5/7) to a port group number (for example, Po80).

For MAC address table entries used by routed ports, the routed port name is displayed in the “vlan” column rather than the internal VLAN number.

Examples This example shows how to display all dynamic MAC address entries:

```
Switch# show mac-address-table dynamic
Unicast Entries
vlan  mac address      type      protocols      port
-----+-----+-----+-----+-----
  1    0000.0000.0201    dynamic  ip              FastEthernet6/15
```

```

1      0000.0000.0202    dynamic ip                               FastEthernet6/15
1      0000.0000.0203    dynamic ip,assigned                      FastEthernet6/15
1      0000.0000.0204    dynamic ip,assigned                      FastEthernet6/15
1      0000.0000.0205    dynamic ip,assigned                      FastEthernet6/15
2      0000.0000.0101    dynamic ip                               FastEthernet6/16
2      0000.0000.0102    dynamic ip                               FastEthernet6/16
2      0000.0000.0103    dynamic ip,assigned                      FastEthernet6/16
2      0000.0000.0104    dynamic ip,assigned                      FastEthernet6/16
2      0000.0000.0105    dynamic ip,assigned                      FastEthernet6/16
Switch#

```

This example shows how to display dynamic MAC address entries with a specific protocol type (in this case, assigned):

```

Switch# show mac-address-table dynamic protocol assigned
Unicast Entries
-----+-----+-----+-----+-----+
vlan  mac address      type      protocols      port
-----+-----+-----+-----+-----+
1      0000.0000.0203    dynamic  ip,assigned    FastEthernet6/15
1      0000.0000.0204    dynamic  ip,assigned    FastEthernet6/15
1      0000.0000.0205    dynamic  ip,assigned    FastEthernet6/15
2      0000.0000.0103    dynamic  ip,assigned    FastEthernet6/16
2      0000.0000.0104    dynamic  ip,assigned    FastEthernet6/16
2      0000.0000.0105    dynamic  ip,assigned    FastEthernet6/16
Switch#

```

Related Commands

[show mac-address-table protocol](#)
[show mac-address-table static](#)
[show mac-address-table vlan](#)

show mac-address-table interface

To display the MAC address table information for a specific interface, use the **show mac-address-table interface** command.

show mac-address-table interface *type slot/port*

Syntax Description

<i>type</i>	Interface type; valid values are Ethernet , FastEthernet , and GigabitEthernet .
<i>slot/port</i>	Number of the slot and port.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

For MAC address table entries used by routed ports, the routed port name is displayed in the “vlan” column rather than the internal VLAN number.

Examples

This example shows how to display MAC address table information for a specific interface:

```
Switch# show mac-address-table interface fa6/16
Unicast Entries
  vlan  mac address      type      protocols      port
-----+-----+-----+-----+-----
   2    0000.0000.0101    dynamic  other          FastEthernet6/16
   2    0000.0000.0102    dynamic  other          FastEthernet6/16
   2    0000.0000.0103    dynamic  other          FastEthernet6/16
   2    0000.0000.0104    dynamic  other          FastEthernet6/16
   2    0000.0000.0105    dynamic  other          FastEthernet6/16
   2    0000.0000.0106    dynamic  other          FastEthernet6/16

Multicast Entries
  vlan  mac address      type      ports
-----+-----+-----+-----
   2    ffff.ffff.ffff    system  Fa6/16
Switch#
```

Related Commands

show mac-address-table address
show mac-address-table aging-time
show mac-address-table count
show mac-address-table dynamic
show mac-address-table multicast
show mac-address-table protocol
show mac-address-table static
show mac-address-table vlan

show mac-address-table multicast

To display multicast MAC address table information, use the **show mac-address-table multicast** command.

```
show mac-address-table multicast [count | {igmp-snooping [count]} | {user [count]} |
{vlan vlan_num}]
```

Syntax Description	Parameter	Description
	count	(Optional) Displays number of multicast entries.
	igmp-snooping	(Optional) Displays only addresses learned by IGMP snooping.
	user	(Optional) Displays only user-entered static addresses.
	vlan vlan_num	(Optional) Displays information for a specific VLAN only; valid values are from 1 to 4094.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Added support for extended VLAN addresses.

Usage Guidelines For MAC address table entries used by routed ports, the routed port name is displayed in the “vlan” column rather than the internal VLAN number.

Examples This example shows how to display multicast MAC address table information for a specific VLAN:

```
Switch# show mac-address-table multicast vlan 1
Multicast Entries
vlan mac address type ports
-----+-----+-----+-----
1 ffff.ffff.ffff system Switch,Fa6/15
Switch#
```

This example shows how to display the number of multicast MAC entries for all VLANs:

```
Switch# show mac-address-table multicast count
MAC Entries for all vlans:
Multicast MAC Address Count: 141
Total Multicast MAC Addresses Available: 16384
Switch#
```

Related Commands

show mac-address-table address
show mac-address-table aging-time
show mac-address-table count
show mac-address-table dynamic
show mac-address-table interface
show mac-address-table protocol
show mac-address-table static
show mac-address-table vlan

show mac-address-table protocol

To display MAC address table information based on the protocol, use the **show mac-address-table protocol** command.

```
show mac-address-table protocol { assigned | ip | ipx | other }
```

Syntax Description	Parameter	Description
	assigned	Specifies assigned protocol entries.
	ip	Specifies IP protocol entries.
	ipx	Specifies IPX protocol entries.
	other	Specifies other protocol entries.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines For MAC address table entries used by routed ports, the routed port name is displayed in the “vlan” column rather than the internal VLAN number.

Examples This example shows how to display MAC address table entries that have a specific protocol type (in this case, assigned):

```
Switch# show mac-address-table protocol assigned
vlan  mac address      type    protocol  qos      ports
-----+-----+-----+-----+-----+-----
 200  0050.3e8d.6400    static  assigned  --      Switch
 100  0050.3e8d.6400    static  assigned  --      Switch
   5  0050.3e8d.6400    static  assigned  --      Switch
4092  0000.0000.0000    dynamic assigned  --      Switch
   1  0050.3e8d.6400    static  assigned  --      Switch
   4  0050.3e8d.6400    static  assigned  --      Switch
4092  0050.f0ac.3058    static  assigned  --      Switch
4092  0050.f0ac.3059    dynamic assigned  --      Switch
   1  0010.7b3b.0978    dynamic assigned  --      Fa5/9
Switch#
```

This example shows the other output for the previous example:

```
Switch# show mac-address-table protocol other
Unicast Entries
vlan  mac address      type    protocols  port
-----+-----+-----+-----+-----
   1  0000.0000.0201    dynamic other      FastEthernet6/15
   1  0000.0000.0202    dynamic other      FastEthernet6/15
```

```

1      0000.0000.0203    dynamic other           FastEthernet6/15
1      0000.0000.0204    dynamic other           FastEthernet6/15
1      0030.94fc.0dff     static ip,ipx,assigned,other Switch
2      0000.0000.0101    dynamic other           FastEthernet6/16
2      0000.0000.0102    dynamic other           FastEthernet6/16
2      0000.0000.0103    dynamic other           FastEthernet6/16
2      0000.0000.0104    dynamic other           FastEthernet6/16
Fa6/1  0030.94fc.0dff     static ip,ipx,assigned,other Switch
Fa6/2  0030.94fc.0dff     static ip,ipx,assigned,other Switch

```

Multicast Entries

vlan	mac address	type	ports
1	ffff.ffff.ffff	system	Switch,Fa6/15
2	ffff.ffff.ffff	system	Fa6/16
1002	ffff.ffff.ffff	system	
1003	ffff.ffff.ffff	system	
1004	ffff.ffff.ffff	system	
1005	ffff.ffff.ffff	system	
Fa6/1	ffff.ffff.ffff	system	Switch,Fa6/1
Fa6/2	ffff.ffff.ffff	system	Switch,Fa6/2

Switch#

Related Commands

[show mac-address-table address](#)
[show mac-address-table aging-time](#)
[show mac-address-table count](#)
[show mac-address-table dynamic](#)
[show mac-address-table interface](#)
[show mac-address-table multicast](#)
[show mac-address-table static](#)
[show mac-address-table vlan](#)

show mac-address-table static

To display static MAC address table entries only, use the **show mac-address-table static** command.

```
show mac-address-table static [address mac_addr | interface type number | protocol protocol |
vlan vlan_id]
```

Syntax Description	Parameter	Description
	address <i>mac_addr</i>	(Optional) Specifies a 48-bit MAC address to match; the valid format is H.H.H.
	interface <i>type slot/port</i>	(Optional) Specifies an interface to match; valid values for <i>type</i> are FastEthernet and GigabitEthernet .
	protocol <i>protocol</i>	(Optional) Specifies a protocol. See “Usage Guidelines” for more information.
	vlan <i>vlan_id</i>	(Optional) Displays entries for a specific VLAN; valid values are from 1 to 4094.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Added support for extended VLAN addresses.

Usage Guidelines For MAC address table entries used by routed ports, the routed port name is displayed in the “vlan” column rather than the internal VLAN number.

The keyword definitions for the *protocol* argument are as follows:

- **assigned** specifies assigned protocol entries.
- **ip** specifies IP protocol.
- **ipx** specifies IPX protocols.
- **other** specifies other protocol entries.

Examples This example shows how to display all static MAC address entries:

```
Switch# show mac-address-table static
Unicast Entries
  vlan  mac address          type          protocols          port
-----+-----+-----+-----+-----
    1   0030.94fc.0dff        static ip,ipx,assigned,other Switch
Fa6/1   0030.94fc.0dff        static ip,ipx,assigned,other Switch
Fa6/2   0030.94fc.0dff        static ip,ipx,assigned,other Switch
```

```

Multicast Entries
  vlan    mac address    type    ports
-----+-----+-----+-----
      1    ffff.ffff.ffff    system Switch,Fa6/15
      2    ffff.ffff.ffff    system Fa6/16
  1002    ffff.ffff.ffff    system
  1003    ffff.ffff.ffff    system
  1004    ffff.ffff.ffff    system
  1005    ffff.ffff.ffff    system
  Fa6/1    ffff.ffff.ffff    system Switch,Fa6/1
  Fa6/2    ffff.ffff.ffff    system Switch,Fa6/2
  .
  .
Switch#

```

This example shows how to display static MAC address entries with a specific protocol type (in this case, assigned):

```

Switch# show mac-address-table static protocol assigned
Unicast Entries
  vlan    mac address    type    protocols    port
-----+-----+-----+-----+-----
      1    0030.94fc.0dff    static ip,ipx,assigned,other Switch
  Fa6/1    0030.94fc.0dff    static ip,ipx,assigned,other Switch
  Fa6/2    0030.94fc.0dff    static ip,ipx,assigned,other Switch

Multicast Entries
  vlan    mac address    type    ports
-----+-----+-----+-----
      1    ffff.ffff.ffff    system Switch,Fa6/15
      2    ffff.ffff.ffff    system Fa6/16
  1002    ffff.ffff.ffff    system
  1003    ffff.ffff.ffff    system
  1004    ffff.ffff.ffff    system
  1005    ffff.ffff.ffff    system
  Fa6/1    ffff.ffff.ffff    system Switch,Fa6/1
  Fa6/2    ffff.ffff.ffff    system Switch,Fa6/2
Switch#

```

Related Commands

- [show mac-address-table address](#)
- [show mac-address-table aging-time](#)
- [show mac-address-table count](#)
- [show mac-address-table dynamic](#)
- [show mac-address-table interface](#)
- [show mac-address-table multicast](#)
- [show mac-address-table protocol](#)
- [show mac-address-table vlan](#)

show mac-address-table vlan

To display MAC address table information for a specific VLAN, use the **show mac-address-table vlan** command.

```
show mac-address-table [vlan vlan_id] [protocol protocol]
```

Syntax Description	vlan <i>vlan_id</i> (Optional) Displays entries for a specific VLAN; valid values are from 1 to 4094.
	protocol <i>protocol</i> (Optional) Specifies a protocol. See “Usage Guidelines” for more information.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended addressing was added.

Usage Guidelines For MAC address table entries used by routed ports, the routed port name is displayed in the “vlan” column rather than the internal VLAN number.

The keyword definitions for the *protocol* variable are as follows:

- **assigned** specifies assigned protocol entries.
- **ip** specifies IP protocol.
- **ipx** specifies IPX protocols.
- **other** specifies other protocol entries.

Examples This example shows how to display MAC address table information for a specific VLAN:

```
Switch# show mac-address-table vlan 1
Unicast Entries
vlan  mac address      type      protocols      port
-----+-----+-----+-----+-----
  1    0000.0000.0201    dynamic  ip              FastEthernet6/15
  1    0000.0000.0202    dynamic  ip              FastEthernet6/15
  1    0000.0000.0203    dynamic  other           FastEthernet6/15
  1    0000.0000.0204    dynamic  other           FastEthernet6/15
  1    0030.94fc.0dff     static   ip,ipx,assigned,other  Switch

Multicast Entries
vlan  mac address      type      ports
-----+-----+-----+-----
  1    ffff.ffff.ffff     system   Switch, Fa6/15
Switch#
```

This example shows how to display MAC address table information for a specific protocol type:

```
Switch# show mac-address-table vlan 100 protocol other
Unicast Entries
  vlan  mac address      type      protocols      port
-----+-----+-----+-----+-----
   1    0000.0000.0203    dynamic  other          FastEthernet6/15
   1    0000.0000.0204    dynamic  other          FastEthernet6/15
   1    0030.94fc.0dff      static   ip,ipx,assigned,other  Switch

Multicast Entries
  vlan  mac address      type      ports
-----+-----+-----+-----
   1    ffff.ffff.ffff      system   Switch,Fa6/15
Switch#
```

Related Commands

- [show mac-address-table address](#)
- [show mac-address-table aging-time](#)
- [show mac-address-table count](#)
- [show mac-address-table dynamic](#)
- [show mac-address-table interface](#)
- [show mac-address-table multicast](#)
- [show mac-address-table protocol](#)
- [show mac-address-table static](#)

show module

To display module information, use the **show module** command.

show module [*mod* | **all**]

Syntax Description	
<i>mod</i>	(Optional) Number of the module; valid values vary from chassis to chassis.
all	(Optional) Displays information for all modules.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines In the Mod Sub-Module fields in the command output, the **show module** command displays the supervisor engine number but appends the uplink daughter card's module type and information. If the PoE consumed by the module is more than 50 W above the administratively allocated PoE, the "Status" displays as "PwrOver.". If the PoE consumed by the module is more than 50 W above the PoE module limit., the "Status" displays as "PwrFault".

Examples This example shows how to display information for all modules.

This example shows the **show module** command output for a system with inadequate power for all installed modules. The system does not have enough power for Module 5; the "Status" displays it as "PwrDeny".

```
Switch# show module all
Mod  Ports Card Type                               Model                Serial No.
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
 1     2  1000BaseX (GBIC) Supervisor(active)    WS-X4014             JAB054109GH
 2     6  1000BaseX (GBIC)                               WS-X4306             00000110
 3    18  1000BaseX (GBIC)                               WS-X4418             JAB025104WK
 5     0  Not enough power for module                WS-X4148-FX-MT      00000000000
 6    48  10/100BaseTX (RJ45)                          WS-X4148             JAB023402RP

M MAC addresses                               Hw  Fw      Sw      Status
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
 1 005c.9d1a.f9d0 to 005c.9d1a.f9df 0.5 12.1(11br)EW 12.1(20020313:00  Ok
 2 0010.7bab.9920 to 0010.7bab.9925 0.2                               Ok
 3 0050.7356.2b36 to 0050.7356.2b47 1.0                               Ok
 5 0001.64fe.a930 to 0001.64fe.a95f 0.0                               PwrDeny
 6 0050.0f10.28b0 to 0050.0f10.28df 1.0                               Ok
Switch#
```


This example shows how to display information for a specific module:

```
Switch# show module 2
Mod Ports Card Type                               Model                               Serial No.
-----
  2     2 Catalyst 4000 supervisor 2 (Active)   WS-X6K-SUP2-2GE                     SAD04450LF1
Mod MAC addresses                               Hw  Fw                               Sw                               Status
-----
  2 0001.6461.39c0 to 0001.6461.39c1  1.1 6.1(3)                          6.2(0.97)                        Ok
Mod Sub-Module                               Model                               Serial                               Hw                               Status
-----
  2 Policy Feature Card 2                   WS-F6K-PFC2                         SAD04440HVU                       1.0                               Ok
  2 Cat4k MSFC 2 daughterboard             WS-F6K-MSFC2                       SAD04430J9K                       1.1                               Ok
Switch#
```

show monitor

To display SPAN session information, use the **show monitor** command.

show monitor [**session**] [**range** *session-range* | **local** | **remote** | **all** | *session-number*] [**detail**]

Syntax Description	
session	(Optional) Displays SPAN information for a session.
range	(Optional) Displays information for a range of sessions.
<i>session-range</i>	(Optional) Specifies a range of sessions.
local	(Optional) Displays all local SPAN sessions.
remote	(Optional) Displays RSPAN source and destination sessions.
all	(Optional) Displays SPAN and RSPAN sessions.
<i>session-number</i>	(Optional) Specifies a session number; valid values are from 1 to 6.
detail	(Optional) Displays detailed SPAN information for a session.

Defaults The **detail** keyword only displays lines with a nondefault configuration.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(13)EW	Added support for differing directions within a single user session.
	12.1(19)EW	Output enhanced to display configuration status of SPAN enhancements.
	12.1(20)EW	Added support to display configuration state for remote SPAN and learning.

Examples This example shows how to display SPAN information for session 2:

```
Switch# show monitor session 2
Session 2
-----
Type : Remote Source Session
Source Ports:
    RX Only:      Fa1/1-3
Dest RSPAN VLAN: 901
Ingress : Enabled, default VLAN=2
Learning : Disabled
Switch#
```

This example shows how to display detailed SPAN information for session 1:

```
Switch# show monitor session 1 detail
Session 1
-----
Type           : Local Session
Source Ports   :
    RX Only    : None
```

```
TX Only      : None
Both         : Gi1/1, CPU
Source VLANs :
RX Only      : None
TX Only      : None
Both         : None
Source RSPAN VLAN : Fa6/1
Destination Ports : Fa6/1
Encapsulation : DOT1Q
  Ingress : Enabled, default VLAN = 2
Filter VLANs : None
  Filter Types RX : Good
  Filter Types TX : None
Dest Rspan Vlan : 901
Ingress : Enabled, default VLAN=2
Learning : Disabled
Switch#
```

This example shows how to display SPAN information for session 1 beginning with the line that starts with Destination:

```
Switch# show monitor session 1 | begin Destination
Destination Ports: None
Filter VLANs:      None
Switch#
Switch#
```

Related Commands [monitor session](#)

show pagp

To display port channel information, use the **show pagp** command.

```
show pagp [group-number] {counters | internal | neighbor}
```

Syntax Description	
<i>group-number</i>	(Optional) Channel group number; valid values are from 1 to 64.
counters	Specifies traffic counter information.
internal	Specifies PAgP internal information.
neighbor	Specifies PAgP neighbor information.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines You can enter any **show pagp** command to display the active PAgP port channel information. To display the nonactive information, enter the **show pagp** command with a group.

Examples This example shows how to display PAgP counter information:

```
Switch# show pagp counters
          Information          Flush
Port      Sent   Recv    Sent   Recv
-----
Channel group: 1
  Fa5/4    2660  2452    0      0
  Fa5/5    2676  2453    0      0
Channel group: 2
  Fa5/6    289   261     0      0
  Fa5/7    290   261     0      0
Switch#
```

This example shows how to display internal PAgP information:

```
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  Partner  PAgP  Learning  IfIndx
Fa5/4    SC   U6/S7   30s    30s    1        128   Any       129
```

```

Fa5/5    SC    U6/S7          30s    1    128    Any    129
Switch#

```

This example shows how to display PAGP neighbor information for all neighbors:

```
Switch# show pagp neighbor
```

```

Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.        P - Device learns on physical port.

```

```
Channel group 1 neighbors
```

Port	Partner Name	Partner Device ID	Partner Port	Age	Partner Flags	Partner Group
Fa5/4	JAB031301	0050.0f10.230c	2/45	2s	SAC	2D
Fa5/5	JAB031301	0050.0f10.230c	2/46	27s	SAC	2D

```
Channel group 2 neighbors
```

Port	Partner Name	Partner Device ID	Partner Port	Age	Partner Flags	Partner Group
Fa5/6	JAB031301	0050.0f10.230c	2/47	10s	SAC	2F
Fa5/7	JAB031301	0050.0f10.230c	2/48	11s	SAC	2F

```
Switch#
```

Related Commands

[pagp learn-method](#)
[pagp port-priority](#)

show policy-map

To display policy map information, use the **show policy-map** command.

show policy-map [*policy_map_name*]

Syntax Description	<i>policy_map_name</i> (Optional) Name of the policy map.
---------------------------	---

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples	This example shows how to display policy map information for all policy maps:
-----------------	---

```
Switch# show policy-map
Policy Map ipp5-policy
  class ipp5
    set ip precedence 6
Switch#
```

This example shows how to display policy map information for a specific policy map:

```
Switch# show policy ipp5-policy
Policy Map ipp5-policy
  class ipp5
    set ip precedence 6
Switch#
```

Related Commands	class-map policy-map show class-map show policy-map interface
-------------------------	--

show policy-map interface

To display statistics and configurations of input and output policies attached to an interface, use the **show policy-map interface** command.

```
show policy-map interface [{FastEthernet interface-number} | {GigabitEthernet
interface-number} | {port-channel number} | {vlan vlan_id}] [input | output]
```

Syntax Description		
FastEthernet <i>interface-number</i>	(Optional)	Specifies the Fast Ethernet 802.3 interface.
GigabitEthernet <i>interface-number</i>	(Optional)	Specifies the Gigabit Ethernet 802.3z interface.
port-channel <i>number</i>	(Optional)	Specifies the port channel.
vlan <i>vlan_id</i>	(Optional)	Specifies the VLAN ID; valid values are from 1 to 4094.
input	(Optional)	Specifies input policies only.
output	(Optional)	Specifies output policies only.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Added support for extended VLAN addresses.

Examples This example shows how to display statistics and configurations of all input and output policies attached to an interface:

```
Switch# show policy-map interface

FastEthernet6/1

  service-policy input:ipp5-policy

    class-map:ipp5 (match-all)
      0 packets
      match:ip precedence 5
      set:
        ip precedence 6

    class-map:class-default (match-any)
      0 packets
      match:any
      0 packets

  service-policy output:ipp5-policy
```

show policy-map interface

```

class-map:ipp5 (match-all)
  0 packets
  match:ip precedence 5
  set:
    ip precedence 6

class-map:class-default (match-any)
  0 packets
  match:any
    0 packets
Switch#

```

This example shows how to display input policy statistics and configurations for a specific interface:

```

Switch# show policy-map interface fastethernet 5/36 input
service-policy input:ipp5-policy

class-map:ipp5 (match-all)
  0 packets
  match:ip precedence 5
  set:
    ip precedence 6

class-map:class-default (match-any)
  0 packets
  match:any
    0 packets
Switch#

```

Related Commands

- [class-map](#)
- [policy-map](#)
- [show class-map](#)
- [show qos](#)

show port-security

To display port security settings for an interface or for the switch, use the **show port-security** command.

show port-security [**address**] [**interface** *interface-id*]

Syntax Description	address	(Optional) Displays all secure MAC addresses for all ports or for a specific port.
	interface <i>interface-id</i>	(Optional) Displays port security settings for a specific interface.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(13)EW	Support for this command was first introduced on the Catalyst 4500 series switch.
	12.2(18)EW	Support was enhanced to display sticky MAC addresses.

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 the *interface-id* value, the **show port-security** 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 the *interface-id* value and the **address** keyword, the **show port-security address interface** 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.

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)
-----
      Fa0/1         11             11             0                 Shutdown
      Fa0/5         15             5              0                 Restrict
      Fa0/11        5              4              0                 Protect
-----

Total Addresses in System :21
Max Addresses limit in System :1024
Switch#
```

This is an example of output from the **show port-security interface fastethernet2/2** command:

```
Switch# show port-security interface fastethernet2/2
Port Security           : Enabled
Port Status            : Secure-up
Violation Mode         : Shutdown
Aging Time             : 20 mins
Aging Type             : Inactivity
SecureStatic Address Aging : Enabled
Maximum MAC Addresses  : 11
Total MAC Addresses    : 11
Configured MAC Addresses : 3
Sticky MAC Addresses   : 0
Last Source Address    : 0000.0000.0000
Security Violation Count : 0
Switch#
```

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
-----  -
1       0001.0001.0001   SecureDynamic       Fa2/1    15 (I)
1       0001.0001.0002   SecureSticky        Fa2/1    15 (I)
1       0001.0001.1111   SecureConfigured    Fa2/1    16 (I)
1       0001.0001.1112   SecureConfigured    Fa2/1    -
1       0001.0001.1113   SecureConfigured    Fa2/1    -
1       0005.0005.0001   SecureConfigured    Fa2/5    23
1       0005.0005.0002   SecureConfigured    Fa2/5    23
1       0005.0005.0003   SecureConfigured    Fa2/5    23
1       0011.0011.0001   SecureConfigured    Fa2/11   25 (I)
1       0011.0011.0002   SecureConfigured    Fa2/11   25 (I)
1       0000.0111.0111   SecureDynamic(Dot1x) Fa6/1    -

-----
Total Addresses in System :11
Max Addresses limit in System :1024
Switch#
```

This is an example of output from the **show port-security interface fastethernet2/5 address** command:

```
Switch# show port-security interface fastethernet2/5 address

Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
-----  -
1       0005.0005.0001   SecureConfigured    Fa0/5    19 (I)
1       0005.0005.0002   SecureConfigured    Fa0/5    19 (I)
1       0005.0005.0003   SecureConfigured    Fa0/5    19 (I)

-----
Total Addresses:3Total Addresses in System :10
Max Addresses limit in System :1024
Switch#
```

Related Commands

[switchport port-security](#)

show power

To display the status of power information, use the **show power** command.

```
show power [available | capabilities | detail | inline {[interface] | consumption default | module
mod} | module | status | supplies]
```

Syntax Description		
available	(Optional)	Displays available system power.
capabilities	(Optional)	Displays individual power supply capabilities.
detail	(Optional)	Displays detailed information on power resources.
inline	(Optional)	Displays PoE status.
<i>interface</i>	(Optional)	Type of interface; the only valid value is FastEthernet .
consumption default	(Optional)	Displays the PoE consumption.
module <i>mod</i>	(Optional)	Displays PoE consumption for the specified module.
module	(Optional)	Displays power consumption for each module.
status	(Optional)	Displays power supply status.
supplies	(Optional)	Displays the number of power supplies needed by the system.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines If a powered device is connected to an interface with external power, the switch does not recognize the powered device. The Device column in the output of the **show power inline** command displays as unknown.

If your port is not capable of supporting Power over Ethernet, you will receive the following error message:

```
Power over Ethernet not supported on interface Admin
```

The **show power in-line** *interface* | *module* command displays the amount of power used to operate a Cisco 7960 IP Phone. To view the amount of power requested, use the **show cdp neighbors** command.

Because of the PoE consumed by FPGAs and other hardware components on the module the operating PoE consumption for an 802.3af-compliant module can be nonzero, even when there are no powered devices attached to the module. The operating PoE can vary by as much as 20 watts because of fluctuations in the PoE consumed by the hardware components.

Examples

This example shows how to display general power supply information:

```
Switch# show power
Power
Supply Model No          Type          Status          Fan      Inline
-----
PS1     PWR-C45-2800AC         AC 2800W      good           good     good
PS2     PWR-C45-1000AC         AC 1000W      err-disable    good     n.a.

*** Power Supplies of different type have been detected***

Power supplies needed by system   :1
Power supplies currently available :1

Power Summary
(in Watts)          Used          Maximum
-----
System Power (12V)   328           1360
Inline Power (-50V)  0             1400
Backplane Power (3.3V) 10            40
-----
Total Used           338 (not to exceed Total Maximum Available = 750)
Switch#
```

This example shows how to display the amount of available system power:

```
Switch# show power available
Power Summary
(in Watts)  Available  Used  Remaining
-----
System Power   1360      280   1080
Inline Power   1400       0    1400
Maximum Power  2800      280   2520
Switch#
```

This example shows how to display the detailed information for system power.

```
Switch# show power detail
Power
Supply Model No          Type          Status          Fan      Inline
-----
PS1     PWR-C45-1300ACV        AC 1300W      good           good     good
PS2     none                   --           --            --       --

Power supplies needed by system   :1
Power supplies currently available :1

Power Summary
(in Watts)          Used          Maximum
-----
System Power (12V)   518           1000
Inline Power (-50V)  24            742
Backplane Power (3.3V) 40            40
-----
Total Used           582 (not to exceed Total Maximum Available = 1300)

                                Watts Used of System Power (12V)
                                currently out of reset in reset
-----
Mod  Model
-----
1    WS-X4013+          110          110          110
3    WS-X4448-GB-LX    90           90           50
4    WS-X4418          80           80           50
5    WS-X4248-RJ45V    65           65           25
```

6	WS-X4248-RJ45V	65	65	25
7	WS-4548-GB-RJ45	58	58	15
--	Fan Tray	50	--	--

	Total	518	468	275

Mod	Model	Inline Power Admin		Inline Power Oper		Efficiency
		PS	Device	PS	Device	
1	WS-X4013+	-	-	-	-	-
3	WS-X4448-GB-LX	-	-	-	-	-
4	WS-X4418	-	-	-	-	-
5	WS-X4248-RJ45V	24	22	22	20	89
6	WS-X4248-RJ45V	0	0	22	20	89
7	WS-4548-GB-RJ45	-	-	-	-	-

	Total	24	22	44	40	

**Note**

The “Inline Power Oper” displays the PoE consumed by the powered devices attached to the module in addition to the PoE consumed by the FPGAs and other hardware components on the module. The “Inline Power Admin” displays only the PoE allocated by the powered devices attached to the module.

This example shows how to display the power status information:

```
Switch# show power status
Power
Supply Model No          Type          Status          Fan Sensor      Inline Status
-----
PS1     PWR-C45-2800AC        AC 2800W      good            good           good           good
PS2     PWR-C45-2800AC        AC 2800W      good            good           good           good

Power Supply   Max   Min   Max   Min   Absolute
(Nos in Watts) Inline Inline System System Maximum
-----
PS1             1400 1400 1360 1360 2800
PS2             1400 1400 1360 1360 2800
Switch#
```

This example shows how to verify the PoE consumption for the switch:

```
Switch# show power inline consumption default
Default PD consumption : 5000 mW
Switch#
```

This example shows how to display the status of inline power:

```
Switch# show power inline
Available:677(w) Used:117(w) Remaining:560(w)

Interface Admin Oper          Power(Watts) Device          Class
          From PS   To Device
-----
Fa3/1     auto  on           17.3    15.4    Ieee PD         0
Fa3/2     auto  on            4.5     4.0    Ieee PD         1
Fa3/3     auto  on            7.1     6.3    Cisco IP Phone 7960 0
Fa3/4     auto  on            7.1     6.3    Cisco IP Phone 7960 n/a
Fa3/5     auto  on           17.3    15.4    Ieee PD         0
Fa3/6     auto  on           17.3    15.4    Ieee PD         0
Fa3/7     auto  on            4.5     4.0    Ieee PD         1
Fa3/8     auto  on            7.9     7.0    Ieee PD         2
Fa3/9     auto  on           17.3    15.4    Ieee PD         3
Fa3/10    auto  on           17.3    15.4    Ieee PD         4
```

show power

```

Fa3/11    auto    off      0        0        n/a      n/a
Fa3/12    auto    off      0        0        n/a      n/a
Fa3/13    auto    off      0        0        n/a      n/a
Fa3/14    auto    off      0        0        n/a      n/a
Fa3/15    auto    off      0        0        n/a      n/a
Fa3/16    auto    off      0        0        n/a      n/a
Fa3/17    auto    off      0        0        n/a      n/a
Fa3/18    auto    off      0        0        n/a      n/a

```

```
-----
Totals:          10    on    117.5    104.6

```

```
Switch#
```

This example shows how to display the number of power supplies needed by the system:

```

Switch# show power supplies
Power supplies needed by system = 2
Switch#

```

This example shows how to display the PoE status for Fast Ethernet interface 3/1:

```

Switch# show power inline fa3/1
Available:677(w) Used:11(w) Remaining:666(w)

```

Interface	Admin	Oper	Power(Watts)		Device	Class
			From PS	To Device		
Fa3/1	auto	on	11.2	10.0	Ieee PD	0

Interface	AdminPowerMax (Watts)	AdminConsumption (Watts)
Fa3/1	15.4	10.0

```
Switch#
```

Related Commands

[power dc input](#)
[power inline](#)
[power inline consumption](#)
[power redundancy-mode](#)
[power supplies required](#)

show qos

To display QoS information, use the **show qos** command.

show qos

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows the output that might be displayed if you do not enter any keywords:

```
Switch# show qos
  QoS is enabled globally
Switch#
```

Related Commands [qos \(global configuration mode\)](#)
[qos \(interface configuration mode\)](#)

show qos aggregate policer

To display QoS aggregate policer information, use the **show qos aggregate policer** command.

show qos aggregate policer [*aggregate_name*]

Syntax Description	<i>aggregate_name</i> (Optional) Named aggregate policer.
---------------------------	---

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	The aggregate policer name is case sensitive.
-------------------------	---

Examples	This example shows the output if you do not enter any keywords:
-----------------	---

```
Switch# show qos aggregate policer
Policer aggr-1
Rate(bps):10000000 Normal-Burst(bytes):1000000
conform-action:transmit exceed-action:policed-dscp-transmit
Policymaps using this policer:
    ipp5-policy
Switch#
```

Related Commands	qos aggregate-policer
-------------------------	---------------------------------------

show qos dbl

To display global Dynamic Buffer Limiting (DBL) information, use the **show qos dbl** command.

show qos dbl

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to display global DBL information:

```
Switch# show qos dbl
DBL is enabled globally
DBL flow includes vlan
DBL flow includes l4-ports
DBL does not use ecn to indicate congestion
DBL exceed-action mark probability:15%
DBL max credits:15
DBL aggressive credit limit:10
DBL aggressive buffer limit:2 packets
Switch#
```

Related Commands [qos \(global configuration mode\)](#)
[qos dbl](#)

show qos interface

To display queueing information, use the **show qos interface** command.

```
show qos interface {FastEthernet interface-number | GigabitEthernet interface-number} |
[vlan vlan_id | port-channel number]
```

Syntax Description		
FastEthernet <i>interface-number</i>		Specifies the Fast Ethernet 802.3 interface.
GigabitEthernet <i>interface-number</i>		Specifies the Gigabit Ethernet 802.3z interface.
vlan <i>vlan_id</i>		(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.
port-channel <i>number</i>		(Optional) Specifies the port channel; valid ranges are from 1 to 64.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(13)EW	Added support for extended VLAN addresses.
	12.1(19)EW	Display changed to include the Port Trust Device.

Examples This example shows how to display queueing information:

```
Switch# show qos interface fastethernet 6/1
  QoS is enabled globally
  Port QoS is enabled
  Administrative Port Trust State: 'dscp'
  Operational Port Trust State: 'untrusted'
  Port Trust Device: 'cisco-phone'
  Default DSCP:0 Default CoS:0

  Tx-Queue   Bandwidth   ShapeRate   Priority   QueueSize
             (bps)       (bps)
  1           31250000    disabled    N/A       240
  2           31250000    disabled    N/A       240
  3           31250000    disabled    normal    240
  4           31250000    disabled    N/A       240
Switch#
```

Related Commands

- [qos map cos](#)
- [show qos](#)
- [tx-queue](#)

show qos maps

To display QoS map information, use the **show qos maps** command.

show qos maps [cos | dscp [policed | tx-queue]]

Syntax Description	
cos	(Optional) Displays CoS map information.
dscp	(Optional) Displays DSCP map information.
policed	(Optional) Displays policed map information.
tx-queue	(Optional) Displays tx-queue map information.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to display QoS map settings:

```
Switch# show qos maps
DSCP-TxQueue Mapping Table (dscp = dld2)
dl :d2  0  1  2  3  4  5  6  7  8  9
-----
0 :    01 01 01 01 01 01 01 01 01 01
1 :    01 01 01 01 01 01 02 02 02 02
2 :    02 02 02 02 02 02 02 02 02 02
3 :    02 02 03 03 03 03 03 03 03 03
4 :    03 03 03 03 03 03 03 03 04 04
5 :    04 04 04 04 04 04 04 04 04 04
6 :    04 04 04 04

Policed DSCP Mapping Table (dscp = dld2)
dl :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
```

■ show qos maps

```
DSCP-CoS Mapping Table (dscp = d1d2)
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 Mapping Table
CoS:  0  1  2  3  4  5  6  7
-----
DSCP:  0  8 16 24 32 40 48 56
```

Switch#

Related Commands

qos (global configuration mode)
qos (interface configuration mode)

show redundancy

To display redundancy facility information, use the **show redundancy** command.

show redundancy { clients | counters | history | states }

Syntax Description		
clients	Displays the redundancy facility client information.	
counters	Displays the redundancy facility counter information.	
history	Displays a log of past status and related information for the redundancy facility.	
states	Displays the redundancy facility state information.	

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1.(13)EW	Support for this command was introduced on the Catalyst 4500 series switch (Catalyst 4507R only.)

Examples This example shows how to display redundancy facility client information:

```
Switch# show redundancy clients
clientID = 0      clientSeq = 0      RF_INTERNAL_MSG
clientID = 30    clientSeq = 135    Redundancy Mode RF
clientID = 28    clientSeq = 330    GALIOS_CONFIG_SYNC
clientID = 65000 clientSeq = 65000 RF_LAST_CLIENT Switch
```

The output displays the following information:

- clientID displays the client's ID number.
- clientSeq displays the client's notification sequence number.
- Current redundancy facility state.

This example shows how to display the redundancy facility counter information:

```
Switch# show redundancy counters
Redundancy Facility OMs
      comm link up = 1
      comm link down down = 0

      invalid client tx = 0
      null tx by client = 0
      tx failures = 0
      tx msg length invalid = 0

      client not rxing msgs = 0
      rx peer msg routing errors = 0
      null peer msg rx = 0
```

show redundancy

```

        errored peer msg rx = 0
            buffers tx = 1535
tx buffers unavailable = 0
            buffers rx = 1530
        buffer release errors = 0

duplicate client registers = 0
failed to register client = 0
Invalid client syncs = 0

```

This example shows how to display redundancy facility history information:

```

Switch# show redundancy history
00:00:01 client added: RF_INTERNAL_MSG(0) seq=0
00:00:01 client added: RF_LAST_CLIENT(65000) seq=65000
00:00:01 client added: GALIOS_CONFIG_SYNC(28) seq=330
00:00:03 client added: Redundancy Mode RF(30) seq=135
00:00:03 *my state = INITIALIZATION(2) *peer state = DISABLED(1)
00:00:03 RF_PROG_INITIALIZATION(100) RF_INTERNAL_MSG(0) op=0 rc=11
00:00:03 RF_PROG_INITIALIZATION(100) Redundancy Mode RF(30) op=0 rc=11
00:00:03 RF_PROG_INITIALIZATION(100) GALIOS_CONFIG_SYNC(28) op=0 rc=11
00:00:03 RF_PROG_INITIALIZATION(100) RF_LAST_CLIENT(65000) op=0 rc=11
00:00:03 *my state = NEGOTIATION(3) peer state = DISABLED(1)
00:00:25 RF_EVENT_GO_ACTIVE(511) op=0
00:00:25 *my state = ACTIVE-FAST(9) peer state = DISABLED(1)
00:00:25 RF_STATUS_MAINTENANCE_ENABLE(403) Redundancy Mode RF(30) op=0
00:00:25 RF_STATUS_MAINTENANCE_ENABLE(403) GALIOS_CONFIG_SYNC(28) op=0
00:00:25 RF_PROG_ACTIVE_FAST(200) RF_INTERNAL_MSG(0) op=0 rc=11
00:00:25 RF_PROG_ACTIVE_FAST(200) Redundancy Mode RF(30) op=0 rc=11
00:00:25 RF_PROG_ACTIVE_FAST(200) GALIOS_CONFIG_SYNC(28) op=0 rc=11
00:00:25 RF_PROG_ACTIVE_FAST(200) RF_LAST_CLIENT(65000) op=0 rc=11
00:00:25 *my state = ACTIVE-DRAIN(10) peer state = DISABLED(1)
00:00:25 RF_PROG_ACTIVE_DRAIN(201) RF_INTERNAL_MSG(0) op=0 rc=11
00:00:25 RF_PROG_ACTIVE_DRAIN(201) Redundancy Mode RF(30) op=0 rc=11
00:00:25 RF_PROG_ACTIVE_DRAIN(201) GALIOS_CONFIG_SYNC(28) op=0 rc=11
00:00:25 RF_PROG_ACTIVE_DRAIN(201) RF_LAST_CLIENT(65000) op=0 rc=11
---cut---cut---cut---
---cut---cut---cut---
00:01:34 RF_PROG_PLATFORM_SYNC(300) RF_INTERNAL_MSG(0) op=0 rc=11
00:01:34 RF_PROG_PLATFORM_SYNC(300) Redundancy Mode RF(30) op=0 rc=11
00:01:34 RF_PROG_PLATFORM_SYNC(300) GALIOS_CONFIG_SYNC(28) op=0 rc=0
00:01:34 RF_EVENT_CLIENT_PROGRESSION(503) GALIOS_CONFIG_SYNC(28) op=1 rc=0
00:01:36 RF_EVENT_PEER_PROG_DONE(506) GALIOS_CONFIG_SYNC(28) op=300
00:01:36 RF_PROG_PLATFORM_SYNC(300) RF_LAST_CLIENT(65000) op=0 rc=0
00:01:36 RF_EVENT_CLIENT_PROGRESSION(503) RF_LAST_CLIENT(65000) op=1 rc=0
00:01:36 RF_EVENT_PEER_PROG_DONE(506) RF_LAST_CLIENT(65000) op=300
00:01:38 *my state = ACTIVE(13) *peer state = STANDBY COLD(4)

```

This example shows how to display redundancy facility state information:

```

Switch# show redundancy state
my state = 13 -ACTIVE
peer state = 4 -STANDBY COLD
Mode = Duplex
Unit = Primary
Unit ID = 1

Redundancy Mode (Operational) = RPR
Redundancy Mode (Configured) = RPR
Split Mode = Disabled
Manual Swact = Enabled
Communications = Up

```

```
client count = 4
client_notification_TMR = 30000 milliseconds
  keep_alive TMR = 4000 milliseconds
    keep_alive count = 1
    keep_alive threshold = 7
      RF debug mask = 0x0
Switch#
```

Related Commands

[redundancy](#)
[redundancy force-switchover](#)

show running-config

To display module status and configuration, use the **show running-config** command.

show running-config [**module slot**]

Syntax Description	module slot (Optional) Specifies the module slot number; valid values are from 1 to 6.				
Defaults	This command has no default settings.				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(8a)EW</td> <td>Support for this command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Release	Modification				
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.				

Usage Guidelines

In some cases, you might see a difference in the duplex mode displayed when you enter the **show interfaces** command and the **show running-config** command. If you do see a difference, the duplex mode displayed in the **show interfaces** command is the actual duplex mode the interface is running. The **show interfaces** command shows the operating mode for an interface, while the **show running-config** command shows the configured mode for an interface.

The **show running-config** command output for an interface may display a duplex mode configuration but no configuration for the speed. When no speed is displayed in the output, it indicates that the interface speed is configured to be auto and that the duplex mode shown becomes the operational setting once the speed is configured to something other than auto. With this configuration, it is possible that the operating duplex mode for that interface does not match the duplex mode shown with the **show running-config** command.

Examples

This example shows how to display module and status configuration for all modules:

```
Switch# show running-config
03:23:36:%SYS-5-CONFIG_I:Configured from console by consolesh runn
Building configuration...

Current configuration:3268 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
!
power supplies required 1
ip subnet-zero
```



```
!  
!  
!  
interface FastEthernet1  
  no ip address  
  shutdown  
  duplex auto  
  speed auto  
Switch#
```

This example shows the output for the **show running-config** command when you have enabled the **switchport voice vlan** command:

```
Switch# show running-config int fastethernet 6/1  
Building configuration...  
  
Current configuration:133 bytes  
!  
interface FastEthernet6/1  
  switchport voice vlan 2  
  no snmp trap link-status  
  spanning-tree portfast  
  channel-group 1 mode on  
end  
  
Switch#
```

■ show slavebootflash:

show slavebootflash:

To display information about the standby bootflash file system, use the **show slavebootflash:** command.

show slavebootflash: [all | chips | fileys]

Syntax Description	all	(Optional) Displays all possible Flash information.
	chips	(Optional) Displays Flash chip information.
	fileys	(Optional) Displays file system information.

Defaults This command has no default settings.

Command Modes EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to display file system status information:

```
Switch> show slavebootflash: fileys

----- F I L E   S Y S T E M   S T A T U S -----
Device Number = 0
DEVICE INFO BLOCK: bootflash
  Magic Number      = 6887635   File System Vers = 10000   (1.0)
  Length            = 1000000   Sector Size      = 40000
  Programming Algorithm = 39     Erased State     = FFFFFFFF
  File System Offset = 40000    Length           = F40000
  MONLIB Offset     = 100       Length           = C628
  Bad Sector Map Offset = 3FFF8   Length           = 8
  Squeeze Log Offset = F80000   Length           = 40000
  Squeeze Buffer Offset = FC0000  Length           = 40000
  Num Spare Sectors = 0
  Spares:
STATUS INFO:
  Writable
  NO File Open for Write
  Complete Stats
  No Unrecovered Errors
  No Squeeze in progress
USAGE INFO:
  Bytes Used      = 917CE8   Bytes Available = 628318
  Bad Sectors    = 0        Spared Sectors  = 0
  OK Files       = 2        Bytes           = 917BE8
  Deleted Files  = 0        Bytes           = 0
  Files w/Errors = 0        Bytes           = 0
Switch>
```

This example shows how to display system image information:

```
Switch> show slavebootflash:
-# - ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
1  .. image      8C5A393A  237E3C   14  2063804 Aug 23 1999 16:18:45 c4-boot-mz
2  .. image      D86EE0AD  957CE8    9  7470636 Sep 20 1999 13:48:49 rp.halley
Switch>
```

This example shows how to display all bootflash information:

```
Switch> show slavebootflash: all
-# - ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
1  .. image      8C5A393A  237E3C   14  2063804 Aug 23 1999 16:18:45 c4-boot-
mz
2  .. image      D86EE0AD  957CE8    9  7470636 Sep 20 1999 13:48:49 rp.halley

6456088 bytes available (9534696 bytes used)

----- F I L E   S Y S T E M   S T A T U S -----
Device Number = 0
DEVICE INFO BLOCK: bootflash
Magic Number      = 6887635   File System Vers = 10000   (1.0)
Length            = 1000000   Sector Size      = 40000
Programming Algorithm = 39   Erased State     = FFFFFFFF
File System Offset = 40000   Length = F40000
MONLIB Offset     = 100     Length = C628
Bad Sector Map Offset = 3FFF8   Length = 8
Squeeze Log Offset = F80000  Length = 40000
Squeeze Buffer Offset = FC0000  Length = 40000
Num Spare Sectors = 0
Spares:
STATUS INFO:
Writable
NO File Open for Write
Complete Stats
No Unrecovered Errors
No Squeeze in progress
USAGE INFO:
Bytes Used      = 917CE8   Bytes Available = 628318
Bad Sectors    = 0       Spared Sectors = 0
OK Files       = 2       Bytes = 917BE8
Deleted Files  = 0       Bytes = 0
Files w/Errors = 0       Bytes = 0
Switch>
```

■ show slaveslot0:

show slaveslot0:

To display information about the file system on the standby supervisor engine, use the **show slaveslot0:** command.

show slot0: [all | chips | filesys]

Syntax Description	all	(Optional) Displays all Flash information including the output from the show slot0: chips and show slot0: filesys commands.
	chips	(Optional) Displays Flash chip register information.
	filesys	(Optional) Displays file system status information.

Defaults This command has no default settings.

Command Modes EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to display a summary of the file system:

```
Switch> show slaveslot0:
-# - ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
1  .. image    6375DBB7  A4F144    6 10678468 Nov 09 1999 10:50:42 halley

5705404 bytes available (10678596 bytes used)
Switch>
```

This example shows how to display Flash chip information:

```
Switch> show slaveslot0: chips
***** Intel Series 2+ Status/Register Dump *****
ATTRIBUTE MEMORY REGISTERS:
  Config Option Reg (4000): 2
  Config Status Reg (4002): 0
  Card Status Reg (4100): 1
  Write Protect Reg (4104): 4
  Voltage Cntrl Reg (410C): 0
  Rdy/Busy Mode Reg (4140): 2

COMMON MEMORY REGISTERS: Bank 0
Intelligent ID Code : 8989A0A0
Compatible Status Reg: 8080
Global Status Reg: B0B0
Block Status Regs:
  0 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
  8 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
 16 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
 24 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
```

```

COMMON MEMORY REGISTERS: Bank 1
  Intelligent ID Code : 8989A0A0
  Compatible Status Reg: 8080
  Global      Status Reg: B0B0
  Block Status Regs:
    0 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
    8 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   16 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   24 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0

COMMON MEMORY REGISTERS: Bank 2
  Intelligent ID Code : 8989A0A0
  Compatible Status Reg: 8080
  Global      Status Reg: B0B0
  Block Status Regs:
    0 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
    8 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   16 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   24 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0

COMMON MEMORY REGISTERS: Bank 3
  Intelligent ID Code : 8989A0A0
  Compatible Status Reg: 8080
  Global      Status Reg: B0B0
  Block Status Regs:
    0 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
    8 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   16 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   24 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0

COMMON MEMORY REGISTERS: Bank 4
  Intelligent ID Code : FFFFFFFF
  IID Not Intel -- assuming bank not populated

```

This example shows how to display file system information:

```

Switch> show slaveslot0: filesystems
----- F I L E   S Y S T E M   S T A T U S -----
  Device Number = 0
DEVICE INFO BLOCK: slot0
  Magic Number      = 6887635   File System Vers = 10000   (1.0)
  Length            = 1000000   Sector Size      = 20000
  Programming Algorithm = 4     Erased State     = FFFFFFFF
  File System Offset = 20000    Length = FA0000
  MONLIB Offset     = 100       Length = F568
  Bad Sector Map Offset = 1FFF0  Length = 10
  Squeeze Log Offset = FC0000   Length = 20000
  Squeeze Buffer Offset = FE0000 Length = 20000
  Num Spare Sectors = 0
  Spares:
STATUS INFO:
  Writable
  NO File Open for Write
  Complete Stats
  No Unrecovered Errors
  No Squeeze in progress
USAGE INFO:
  Bytes Used      = 9F365C   Bytes Available = 5AC9A4
  Bad Sectors     = 0        Spared Sectors  = 0
  OK Files        = 1        Bytes = 9F35DC
  Deleted Files   = 0        Bytes = 0
  Files w/Errors  = 0        Bytes =
Switch>

```

■ show slot0:

show slot0:

To display information about the slot0: file system, use the **show slot0:** command.

show slot0: [**all** | **chips** | **filesys**]

Syntax Description	all	(Optional) Displays all Flash information including the output from the show slot0: chips and show slot0: filesys commands.
	chips	(Optional) Displays Flash chip register information.
	filesys	(Optional) Displays file system status information.

Defaults This command has no default settings.

Command Modes EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to display a summary of the file system:

```
Switch> show slot0:
-# - ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
1  .. image    6375DBB7  A4F144    6 10678468 Nov 09 1999 10:50:42 halley

5705404 bytes available (10678596 bytes used)
Switch>
```

This example shows how to display Flash chip information:

```
Switch> show slot0: chips
***** Intel Series 2+ Status/Register Dump *****
ATTRIBUTE MEMORY REGISTERS:
  Config Option Reg (4000): 2
  Config Status Reg (4002): 0
  Card Status Reg (4100): 1
  Write Protect Reg (4104): 4
  Voltage Cntrl Reg (410C): 0
  Rdy/Busy Mode Reg (4140): 2

COMMON MEMORY REGISTERS: Bank 0
  Intelligent ID Code : 8989A0A0
  Compatible Status Reg: 8080
  Global Status Reg: B0B0
  Block Status Regs:
    0 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
    8 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   16 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   24 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
```

```

COMMON MEMORY REGISTERS: Bank 1
  Intelligent ID Code   : 8989A0A0
  Compatible Status Reg: 8080
  Global      Status Reg: B0B0
  Block Status Regs:
    0  : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
    8  : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   16 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   24 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0

COMMON MEMORY REGISTERS: Bank 2
  Intelligent ID Code   : 8989A0A0
  Compatible Status Reg: 8080
  Global      Status Reg: B0B0
  Block Status Regs:
    0  : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
    8  : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   16 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   24 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0

COMMON MEMORY REGISTERS: Bank 3
  Intelligent ID Code   : 8989A0A0
  Compatible Status Reg: 8080
  Global      Status Reg: B0B0
  Block Status Regs:
    0  : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
    8  : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   16 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   24 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0

COMMON MEMORY REGISTERS: Bank 4
  Intelligent ID Code   : FFFFFFFF
  IID Not Intel -- assuming bank not populated
Switch>

```

This example shows how to display file system information:

```

Switch> show slot0: fileysys
----- F I L E   S Y S T E M   S T A T U S -----
  Device Number = 0
DEVICE INFO BLOCK: slot0
  Magic Number      = 6887635   File System Vers = 10000   (1.0)
  Length            = 1000000   Sector Size      = 20000
  Programming Algorithm = 4     Erased State     = FFFFFFFF
  File System Offset = 20000    Length = FA0000
  MONLIB Offset     = 100       Length = F568
  Bad Sector Map Offset = 1FFF0  Length = 10
  Squeeze Log Offset = FC0000   Length = 20000
  Squeeze Buffer Offset = FE0000 Length = 20000
  Num Spare Sectors = 0
  Spares:
STATUS INFO:
  Writable
  NO File Open for Write
  Complete Stats
  No Unrecovered Errors
  No Squeeze in progress
USAGE INFO:
  Bytes Used      = 9F365C   Bytes Available = 5AC9A4
  Bad Sectors     = 0        Spared Sectors  = 0
  OK Files        = 1        Bytes = 9F35DC
  Deleted Files   = 0        Bytes = 0
  Files w/Errors  = 0        Bytes = 0
Switch>

```

show spanning-tree

To display spanning tree state information, use the **show spanning-tree** command.

```
show spanning-tree [bridge_group | active | backbonefast | bridge [id] | inconsistentports |
interface type | root | summary [total] | uplinkfast | vlan vlan_id / pathcost method [detail]
```

Syntax Description	
<i>bridge_group</i>	(Optional) Specifies the bridge group number; valid values are from 1 to 255.
active	(Optional) Displays spanning tree information on active interfaces only.
backbonefast	(Optional) Displays spanning tree BackboneFast status.
bridge	(Optional) Displays bridge status and configuration information.
<i>id</i>	(Optional) Name of the bridge.
inconsistentports	(Optional) Displays root inconsistency state.
interface <i>type</i>	(Optional) Specifies the interface type and number; valid values are FastEthernet , GigabitEthernet , port-channel (1 to 64), and vlan (1 to 4094).
root	(Optional) Displays root bridge status and configuration.
summary	(Optional) Specifies a summary of port states.
total	(Optional) Displays the total lines of the spanning tree state section.
uplinkfast	(Optional) Displays spanning tree UplinkFast status.
vlan <i>vlan_id</i>	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.
pathcost method	(Optional) Displays the default path cost calculation method used.
detail	(Optional) Displays a summary of interface information.

Defaults Interface information summary is displayed.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended addressing was added.

Examples This example shows how to display spanning tree information on active interfaces only:

```
Switch# show spanning-tree active
UplinkFast is disabled
BackboneFast is disabled
```

```
VLAN1 is executing the ieee compatible Spanning Tree protocol
Bridge Identifier has priority 32768, address 0050.3e8d.6401
Configured hello time 2, max age 20, forward delay 15
Current root has priority 16384, address 0060.704c.7000
Root port is 265 (FastEthernet5/9), cost of root path is 38
Topology change flag not set, detected flag not set
```



```

Number of topology changes 0 last change occurred 18:13:54 ago
Times: hold 1, topology change 24, notification 2
      hello 2, max age 14, forward delay 10
Timers: hello 0, topology change 0, notification 0

Port 265 (FastEthernet5/9) of VLAN1 is forwarding
Port path cost 19, Port priority 128, Port Identifier 129.9.
Designated root has priority 16384, address 0060.704c.7000
Designated bridge has priority 32768, address 00e0.4fac.b000
Designated port id is 128.2, designated path cost 19
Timers: message age 3, forward delay 0, hold 0
Number of transitions to forwarding state: 1
BPDU: sent 3, received 32852
.
.
.
Switch#

```

This example shows how to display spanning tree BackboneFast status:

```

Switch# show spanning-tree backbonefast
BackboneFast is enabled

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
Switch#

```

This example shows how to display spanning tree information for the bridge:

```

Switch# show spanning-tree bridge
VLAN1
  Bridge ID Priority    32768
           Address     0050.3e8d.6401
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
VLAN2
  Bridge ID Priority    32768
           Address     0050.3e8d.6402
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
VLAN3
  Bridge ID Priority    32768
           Address     0050.3e8d.6403
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
.
.
.
Switch#

```

This example shows how to display a summary of interface information:

```

Switch# show spanning-tree

VLAN1
Spanning tree enabled protocol ieee
Root ID    Priority    32768
Address    0030.94fc.0a00
This bridge is the root
Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID Priority    32768

```

■ show spanning-tree

```

                Address      0030.94fc.0a00
                Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
                Aging Time   300

Interface
Name          Port ID Prio  Cost Sts      Designated
-----
FastEthernet6/15  129.79 128   19 FWD      0 32768 0030.94fc.0a00 129.79

VLAN2
Spanning tree enabled protocol ieee
Root ID      Priority   32768
Address      0030.94fc.0a01
This bridge is the root
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID    Priority   32768
Address      0030.94fc.0a01
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time   300

Interface
Name          Port ID Prio  Cost Sts      Designated
-----
FastEthernet6/16  129.80 128   19 FWD      0 32768 0030.94fc.0a01 129.80
Switch#

```

This example shows how to display spanning tree information for a specific interface:

```

Switch# show spanning-tree interface fastethernet 5/9
Interface Fa0/10 (port 23) in Spanning tree 1 is ROOT-INCONSISTENT
Port path cost 100, Port priority 128
Designated root has priority 8192, address 0090.0c71.a400
Designated bridge has priority 32768, address 00e0.1e9f.8940
Designated port is 23, path cost 115
Timers: message age 0, forward delay 0, hold 0
BPDU: sent 0, received 0
The port is in the portfast mode

```

This example shows how to display spanning tree information for a specific VLAN:

```

Switch# show spanning-tree vlan 1
VLAN1 is executing the ieee compatible Spanning Tree protocol
Bridge Identifier has priority 32768, address 0030.94fc.0a00
Configured hello time 2, max age 20, forward delay 15
We are the root of the spanning tree
Topology change flag not set, detected flag not set
Number of topology changes 5 last change occurred 01:50:47 ago
    from FastEthernet6/16
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

Port 335 (FastEthernet6/15) of VLAN1 is forwarding
    Port path cost 19, Port priority 128, Port Identifier 129.79.
    Designated root has priority 32768, address 0030.94fc.0a00
    Designated bridge has priority 32768, address 0030.94fc.0a00
    Designated port id is 129.79, designated path cost 0
    Timers:message age 0, forward delay 0, hold 0
    Number of transitions to forwarding state:1
    BPDU:sent 6127, received 0
Switch#

```

This example shows how to display spanning tree information for a specific bridge group:

```
Switch# show spanning-tree vlan 1
UplinkFast is disabled
BackboneFast is disabled
```

This example shows how to display a summary of port states:

```
Switch# show spanning-tree summary
Root bridge for:VLAN1, VLAN2.
PortFast BPDU Guard is disabled
EtherChannel misconfiguration guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Default pathcost method used is short

Name                Blocking Listening Learning Forwarding STP Active
-----
VLAN1                0          0          0          1          1
VLAN2                0          0          0          1          1
-----
                2 VLANs 0          0          0          2          2

Switch#
```

This example shows how to display the total lines of the spanning tree state section:

```
Switch# show spanning-tree summary totals
Root bridge for:VLAN1, VLAN2.
PortFast BPDU Guard is disabled
EtherChannel misconfiguration guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Default pathcost method used is short

Name                Blocking Listening Learning Forwarding STP Active
-----
                2 VLANs 0          0          0          2          2

Switch#
```

This example shows how to determine whether any ports are in root inconsistent state:

```
Switch# show spanning-tree inconsistentports

Name                Interface                Inconsistency
-----
VLAN1                FastEthernet3/1          Root Inconsistent

Number of inconsistent ports (segments) in the system:1
Switch#
```

■ show spanning-tree

Related Commands

spanning-tree backbonefast
spanning-tree cost
spanning-tree guard
spanning-tree pathcost method
spanning-tree portfast default
spanning-tree portfast (interface configuration mode)
spanning-tree port-priority
spanning-tree uplinkfast
spanning-tree vlan

show spanning-tree mst

To display MST protocol information, use the **show spanning-tree mst** command.

show spanning-tree mst [**configuration**]

show spanning-tree mst [*instance-id*] [**detail**]

show spanning-tree mst [*instance-id*] **interface** *interface* [**detail**]

Syntax Description	configuration	(Optional) Displays region configuration information.
	<i>instance-id</i>	(Optional) Instance identification number; valid values are from 0 to 15.
	detail	(Optional) Displays detailed MST protocol information.
	interface <i>interface</i>	(Optional) Interface type and number; valid values for type are FastEthernet , GigabitEthernet , port-channel , and vlan . See “Usage Guidelines” for more information.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines This command is not supported on systems configured with a Supervisor Engine 1.

In the output display of the **show spanning-tree mst configuration** command, a warning message might display. This message appears if you do not map secondary VLANs to the same instance as the associated primary VLAN. The display includes a list of the secondary VLANs that are not mapped to the same instance as the associated primary VLAN. The warning message is as follows:

```
These secondary vlans are not mapped to the same instance as their primary:
-> 3
```

See the [show spanning-tree](#) command for output definitions.

Examples This example shows how to display region configuration information:

```
Switch# show spanning-tree mst configuration
Name      [leo]
Revision  2702
Instance  Vlans mapped
-----
0         1-9,11-19,21-29,31-39,41-4094
1         10,20,30,40
-----
```

This example shows how to display additional MST protocol values:

```
Switch# show spanning-tree mst 3 detail
# # # # # MST03 vlans mapped: 3,3000-3999
Bridge address 0002.172c.f400 priority 32771 (32768 sysid 3)
Root this switch for MST03

GigabitEthernet1/1 of MST03 is boundary forwarding
Port info port id 128.1 priority 128
cost 20000
Designated root address 0002.172c.f400 priority 32771
cost 0
Designated bridge address 0002.172c.f400 priority 32771 port
id 128.1
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 4, received 0

FastEthernet4/2 of MST03 is backup blocking
Port info port id 128.194 priority 128 cost
200000
Designated root address 0002.172c.f400 priority 32771
cost 0
Designated bridge address 0002.172c.f400 priority 32771 port id
128.193
Timers: message expires in 2 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 3, received 252
Switch#
```

This example shows how to display MST information for a specific interface:

```
Switch# show spanning-tree mst 0 interface fastEthernet 4/1 detail
Edge port: no (trunk) port guard : none
(default)
Link type: point-to-point (point-to-point) bpdu filter: disable
(default)
Boundary : internal bpdu guard : disable
(default)
FastEthernet4/1 of MST00 is designated forwarding
Vlans mapped to MST00 1-2,4-2999,4000-4094
Port info port id 128.193 priority 128 cost
200000
Designated root address 0050.3e66.d000 priority 8193
cost 20004
Designated ist master address 0002.172c.f400 priority 49152
cost 0
Designated bridge address 0002.172c.f400 priority 49152 port id
128.193
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus sent 492, received 3
Switch#
```

Related Commands

[spanning-tree mst](#)
[spanning-tree mst forward-time](#)
[spanning-tree mst hello-time](#)
[spanning-tree mst max-hops](#)
[spanning-tree mst root](#)

show storm-control

To display broadcast storm control settings on the switch or on the specified interface, use the **show storm-control** user EXEC command.

```
show storm-control [interface-id | broadcast]
```

Syntax Description	<i>interface-id</i>	(Optional) Specifies the interface ID for the physical port.
	broadcast	(Optional) Displays broadcast storm threshold setting.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 broadcast traffic type for all ports on the switch.

Examples This is an example of output from the **show storm-control** command when no keywords are entered. Because no traffic type keyword was entered, the broadcast storm control settings are displayed.

```
Switch# show storm-control
Interface  Filter State  Upper    Lower    Current
-----
Gi2/1     Forwarding    30.00%   30.00%   N/A
Gi4/1     Forwarding    30.00%   30.00%   N/A
Gi4/3     Forwarding    30.00%   30.00%   N/A
```

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 are displayed.

```
Switch# show storm-control fastethernet2/17
Interface  Filter State  Level    Current
-----
Fa2/17     Forwarding    50.00%   0.00%
```

This is an example of output from the **show storm-control** command for a specified interface and traffic type, where no storm control threshold has been set for that traffic type on the specified interface.

```
Switch# show storm-control gigabitethernet2/1 broadcast
Interface  Filter State  Level  Current
-----  -
Gi2/1     forwarding    100.00%  N/A
<output truncated>
```

Table2-18 describes the fields in the **show storm-control** display.

Table2-18 show storm-control Field Descriptions

Field	Description
Interface	Displays the ID of the interface.
Filter State	Displays the status of the filter: <ul style="list-style-type: none"> 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.
Level	Displays the threshold level set on the interface for broadcast traffic.
Current	Displays the bandwidth utilization of broadcast traffic as a percentage of total available bandwidth. This field is only valid when storm control is enabled. Note N/A is displayed for interfaces that do storm control in hardware.

Related Commands

[storm-control](#)
[show interfaces counters](#)
[show running-config](#)

show system mtu

To display the global MTU setting, use the **show system mtu** command.

show system mtu

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to display the global MTU setting:

```
Switch# show system mtu
Global Ethernet MTU is 1550 bytes.
Switch#
```

Related Commands [system mtu](#)

show tech-support

To display troubleshooting information for TAC, use the **show tech-support** command.

show tech-support [**bridging** | **cef** | **ipmulticast** | **isis** | **password** [**page**] | **page**]

Syntax Description	
bridging	(Optional) Specifies bridging-related information.
cef	(Optional) Specifies CEF-related information.
ipmulticast	(Optional) Specifies IP multicast-related information.
isis	(Optional) Specifies CLNS and ISIS-related information.
password	(Optional) Includes passwords and other security information in the output.
page	(Optional) Displays one page of information at a time in the output.

Defaults

The defaults are as follows:

- Outputs are displayed without page breaks.
- Passwords and other security information are removed from the output.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Press the **Return** key to display the next line of output, or press the **Space** bar to display the next page of information. If you do not enter the **page** keyword, the output scrolls. It does not stop for page breaks.

If you enter the **password** keyword, password encryption is enabled, but only the encrypted form appears in the output.

If you do not enter the **password** keyword, passwords and other security-sensitive information in the output are replaced in the output with the word “removed.”

The **show tech-support** commands are a compilation of several **show** commands and the output can be quite lengthy. For a sample display of the output of the **show tech-support** command, see the individual **show** command listed.

If you enter the **show tech-support** command without arguments, the output displays the equivalent of these **show** commands:

- **show version**
- **show running-config**
- **show stacks**
- **show interfaces**
- **show controllers**

- **show process memory**
- **show process cpu**
- **show buffers**
- **show logging**
- **show module**
- **show power**
- **show environment**
- **show interfaces switchport**
- **show interfaces trunk**
- **show vlan**

If you enter the **ipmulticast** keyword, the output displays the equivalent of these **show** commands:

- **show ip pim interface**
- **show ip pim interface count**
- **show ip pim neighbor**
- **show ip pim rp**
- **show ip igmp groups**
- **show ip igmp interface**
- **show ip mroute count**
- **show ip mroute**
- **show ip mcache**
- **show ip dvmrp route**

Examples

For a sample display of the **show tech-support** command output, see the commands listed in “Usage Guidelines” for more information.

Related Commands

See “Usage Guidelines.”

show udld

To display the administrative and operational UDLD status, use the **show udld** command.

show udld *interface-id*

Syntax Description	<i>interface-id</i> Name of the interface.
---------------------------	--

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	If you do not enter an interface ID value, administrative and operational UDLD status for all interfaces is displayed.
-------------------------	--

Examples	This example shows how to display the UDLD state for a single interface:
-----------------	--

```
Switch# show udld GigabitEthernet2/2
Interface Gi2/2
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement
Message interval: 60
Time out interval: 5
No multiple neighbors detected
  Entry 1
  ---
  Expiration time: 146
  Device ID: 1
  Current neighbor state: Bidirectional
  Device name: 0050e2826000
  Port ID: 2/1
  Neighbor echo 1 device: SAD03160954
  Neighbor echo 1 port: Gi1/1
  Message interval: 5
  CDP Device name: 066527791
Switch#
```

Related Commands	udld (global configuration mode) udld (interface configuration mode)
-------------------------	---

show vlan

To display VLAN information, use the **show vlan** command.

```
show vlan [brief | id vlan_id | name name]
```

```
show vlan private-vlan [type]
```

Syntax Description	
brief	(Optional) Displays only a single line for each VLAN, naming the VLAN, status, and ports.
id <i>vlan_id</i>	(Optional) Displays information about a single VLAN identified by VLAN ID number; valid values are from 1 to 4094.
name <i>name</i>	(Optional) Displays information about a single VLAN identified by VLAN name; valid values are an ASCII string from 1 to 32 characters.
private-vlan	Displays private VLAN information.
<i>type</i>	(Optional) Private VLAN type.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Added support for extended VLAN addresses.

Examples This example shows how to display the VLAN parameters for all VLANs within the administrative domain:

```
Switch# show vlan
VLAN Name                Status      Ports
-----
1    default                active     Fa5/9
2    VLAN0002                active     Fa5/9
3    VLAN0003                active     Fa5/9
4    VLAN0004                active     Fa5/9
5    VLAN0005                active     Fa5/9
6    VLAN0006                active     Fa5/9
10   VLAN0010                active     Fa5/9
20   VLAN0020                active     Fa5/9

<...Output truncated...>
```

show vlan

```

850 VLAN0850                active Fa5/9
917 VLAN0917                active Fa5/9
999 VLAN0999                active Fa5/9
1002 fddi-default           active Fa5/9
1003 trcrf-default          active Fa5/9
1004 fddinet-default        active Fa5/9
1005 trbrf-default          active Fa5/9

```

```

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
-----
1 enet 100001 1500 - - - - - 0 0
2 enet 100002 1500 - - - - - 0 0
3 enet 100003 1500 - - - - - 303 0
4 enet 100004 1500 - - - - - 304 0
5 enet 100005 1500 - - - - - 305 0
6 enet 100006 1500 - - - - - 0 0
10 enet 100010 1500 - - - - - 0 0
20 enet 100020 1500 - - - - - 0 0
50 enet 100050 1500 - - - - - 0 0

```

<...Output truncated...>

```

850 enet 100850 1500 - - - - - 0 0
917 enet 100917 1500 - - - - - 0 0
999 enet 100999 1500 - - - - - 0 0
1002 fddi 101002 1500 - 0 - - - 0 0
1003 trcrf 101003 4472 1005 3276 - - srb 0 0
1004 fdnet 101004 1500 - - - - ieee - 0 0
1005 trbrf 101005 4472 - - 15 - ibm - 0 0

```

```
VLAN AREHops STEHops Backup CRF
```

```

-----
802 0 0 off
1003 7 7 off
Switch#

```

This example shows how to display the VLAN name, status, and associated ports only:

```
Switch# show vlan brief
```

```

VLAN Name Status Ports
-----
1 default active Fa5/9
2 VLAN0002 active Fa5/9
3 VLAN0003 active Fa5/9
4 VLAN0004 active Fa5/9
5 VLAN0005 active Fa5/9
10 VLAN0010 active Fa5/9
.
.
.
999 VLAN0999 active Fa5/9
1002 fddi-default active Fa5/9
1003 trcrf-default active Fa5/9
1004 fddinet-default active Fa5/9
1005 trbrf-default active Fa5/9
Switch#

```

This example shows how to display the VLAN parameters for VLAN 3 only:

```
Switch# show vlan id 3
```

```

VLAN Name                Status    Ports
-----
3    VLAN0003                active    Fa5/9

VLAN Type  SAID      MTU    Parent RingNo BridgeNo  Stp  BrdgMode Transl  Trans2
-----
3    enet    100003   1500   -      -        -    -      -      303    0

```

Table2-19 describes the fields in the **show vlan** command output.

Table2-19 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 Identifier 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.

Related Commands

[vlan database](#)
[vlan \(VLAN Database mode\)](#)
[vtp \(global configuration mode\)](#)

show vlan access-map

To display the contents of a VLAN access map, use the **show vlan access-map** command.

show vlan access-map [*map-name*]

Syntax Description	<i>map-name</i> (Optional) Name of the VLAN access map.
---------------------------	---

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples	This command shows how to display the contents of a VLAN access map:
-----------------	--

```
Switch# show vlan access-map mordred
Vlan access-map "mordred" 1
    match: ip address 13
    action: forward capture
Switch#
```

Related Commands	vlan access-map
-------------------------	---------------------------------

show vlan counters

To display software-cached counter values , use the **show vlan counters** command.

show vlan [id *vlanid*] counters

Syntax Description	id <i>vlanid</i> (Optional) Displays the software-cached counter values for a specific VLAN.
---------------------------	---

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst4500 series switches.

Usage Guidelines	If you enter the show vlan counters command without specifying the VLAN ID, software-cached counter values for all VLANs are displayed.
-------------------------	--

Examples	This example shows how to display the software-cached counter values for a specific VLAN:
-----------------	---

```
Switch> show vlan counters
* Multicast counters include broadcast packets

Vlan Id                : 1
L2 Unicast Packets     : 0
L2 Unicast Octets      : 0
L3 Input Unicast Packets : 0
L3 Input Unicast Octets : 0
L3 Output Unicast Packets : 0
L3 Output Unicast Octets : 0
L3 Output Multicast Packets : 0
L3 Output Multicast Octets : 0
L3 Input Multicast Packets : 0
L3 Input Multicast Octets : 0
L2 Multicast Packets   : 1
L2 Multicast Octets    : 94
Switch>
```

Related Commands	clear vlan counters
-------------------------	-------------------------------------

show vlan dot1q tag native

To display all the ports on the switch that are eligible for native VLAN tagging as well as their current native VLAN tagging status, use the **show vlan dot1q tag native** command.

show vlan dot1q tag native

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC

Command History	Release	Modification
	12.1(18)EW	This command was introduced on the Catalyst 4500 series switch.

Examples 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 globally
```

```
Per Port Native Vlan Tagging State
-----
```

Port	Operational Mode	Native VLAN Tagging State
f3/2	trunk	enabled
f3/16	PVLAN trunk	disabled
f3/16	trunk	enabled

Related Commands

- [switchport mode](#)
- vlan (global configuration)** (refer to Cisco IOS documentation)
- vlan (VLAN configuration)** (refer to Cisco IOS documentation)

show vlan internal usage

Use the **show vlan internal usage** command to display information about the internal VLAN allocation.

show vlan [id *vlan-id*] internal usage

Syntax Description	id <i>vlan-id</i> (Optional) Displays internal VLAN allocation information for the specified VLAN; valid values are from 1 to 4094.
---------------------------	--

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Entering the **show vlan internal usage** command displays the OSM interfaces and subinterfaces in addition to the regular Ethernet interfaces.

Examples This example shows how to display information about the current internal VLAN allocation:

```
Switch> show vlan internal usage
```

```
VLAN Usage
-----
1025 -
1026 -
1027 -
1028 -
1029 Port-channel6
1030 GigabitEthernet1/2
1032 FastEthernet3/20
1033 FastEthernet3/21
1129 -
```

This example shows how to display information about the internal VLAN allocation for a specific VLAN:

```
Switch> show vlan id 1030 internal usage
```

```
VLAN Usage
-----
1030 GigabitEthernet1/2
```

Related Commands [vlan internal allocation policy](#)

show vlan mtu

To display the minimum and maximum transmission unit (MTU) sizes of each VLAN, use the **show vlan mtu** command.

show vlan mtu

Syntax Description This command has no arguments or keywords

Defaults This command has no default settings.

Command Modes EXEC

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines The MTU_Mismatch column in the command output indicates whether all the ports in the VLAN have the same MTU. When “yes” is displayed in the MTU_Mismatch column, it means that the VLAN has a port with different MTUs, and packets might be dropped that are switched from a port with a larger MTU to a port with a smaller MTU. If the VLAN does not have an SVI, the hyphen (-) symbol is displayed in the SVI_MTU column.

For a VLAN, if the MTU-Mismatch column displays yes, the names of the port with the MinMTU and the port with the MaxMTU are displayed. For a VLAN, if the SVI_MTU is bigger than the MinMTU, “TooBig” is displayed after the SVI_MTU.

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

```
Switch> show vlan mtu
```

```
VLAN      SVI_MTU      MinMTU(port)  MaxMTU(port)  MTU_Mismatch
-----
1         1500         1500          1500          No
Switch>
```

Related Commands [mtu](#)

show vlan private-vlan

To display PVLAN information, use the **show vlan private-vlan** command.

show vlan private-vlan [type]

Syntax Description	type (Optional) Displays the PVLAN type; valid types are Isolated and Primary.				
Defaults	This command has no default settings.				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(8a)EW</td> <td>Support for this command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Release	Modification				
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.				

Usage Guidelines In the **show vlan private-vlan type** command output when normal is displayed as a type, a regular VLAN has been configured in a PVLAN. When normal is displayed, two VLANs have been associated before type was set and the PVLAN is not operational. This information is useful for debugging purposes.

Examples This example shows how to display all currently configured PVLAN information:

```
Switch# show vlan private-vlan
```

```
Primary Secondary Type Ports
-----
100      101      isolated
150      151      non-operational
401      402      non-operational
Switch#
```

This example shows how to display all currently configured PVLAN type information:

```
Switch# show vlan private-vlan type
```

```
Vlan Type
-----
202 primary
308 normal
440 isolated
Switch#
```

[Table2-20](#) describes the fields in the **show vlan private-vlan** command output.

■ show vlan private-vlan

Table2-20 show vlan private-vlan Command Output Fields

Field	Description
Primary	Number of the primary VLAN.
Secondary	Number of the secondary VLAN.
Secondary-Type	Secondary VLAN type is isolated .
Ports	Indicates the ports within a VLAN.
Type	Type of VLAN; possible values are primary, isolated, or normal .

Related Commands

[private-vlan](#)

[private-vlan mapping](#)

show vlan remote-span

To display a list of Remote SPAN (RSPAN) VLANs, use the **show vlan remote-span** command.

show vlan remote-span

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(12)EW	This command was introduced on the Catalyst4500 series switches.

Examples This example shows how to display a list of RSPAN VLANs:

```
Router# show vlan remote-span
Remote SPAN VLANs
-----
2,20
```

Related Commands [remote-span](#)
[vlan \(VLAN Database mode\)](#)

show vmps

To display the VLAN Query Protocol (VQP) version, reconfirmation interval, retry count, VLAN Membership Policy Server (VMPS) IP addresses, current servers, and primary servers, use the **show vmps** command.

show vmps [statistics]

Syntax Description	statistics (Optional) Displays the client side statistics.
---------------------------	---

Defaults	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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: 172.20.50.120 (primary, current)

Reconfirmation status
-----
VMPS Action:          No Dynamic Port
Switch#
```

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

```
Switch# show vmps statistics
VMPS Client Statistics
-----
VQP  Queries:                0
VQP  Responses:              0
VMPS  Changes:                0
VQP  Shutdowns:              0
VQP  Denied:                  0
VQP  Wrong Domain:           0
VQP  Wrong Version:           0
VQP  Insufficient Resource: 0
Switch#
```

Related Commands	vmps reconfirm (privileged EXEC)
-------------------------	--

show vtp

To display VTP statistics and domain information, use the **show vtp** command.

show vtp { counters | status }

Syntax Description	counters	Specifies VTP statistics.
	status	Specifies VTP domain status.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to display VTP statistics:

```
Switch# show vtp counters
VTP statistics:
Summary advertisements received      : 1
Subset advertisements received      : 1
Request advertisements received     : 0
Summary advertisements transmitted  : 31
Subset advertisements transmitted   : 1
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
-----          -----          -----          -----
Fa5/9          1555          1564          0
Switch#
```

This example shows how to display the VTP domain status:

```
Switch# show vtp status
VTP Version          : 2
Configuration Revision : 250
Maximum VLANs supported locally : 1005
Number of existing VLANs : 33
VTP Operating Mode   : Server
VTP Domain Name      : Lab_Network
VTP Pruning Mode     : Enabled
VTP V2 Mode          : Enabled
VTP Traps Generation : Disabled
```

```

MD5 digest                : 0xE6 0xF8 0x3E 0xDD 0xA4 0xF5 0xC2 0x0E
Configuration last modified by 172.20.52.18 at 9-22-99 11:18:20
Local updater ID is 172.20.52.18 on interface V11 (lowest numbered VLAN interface found)
Switch#

```

This example shows how to display only those lines in the **show vtp** output that contain the word **Summary**:

```

Switch# show vtp counters | include Summary
Summary advertisements received      : 1
Summary advertisements transmitted : 32
Trunk                               Join Transmitted Join Received   Summary advts received from
Switch#

```

[Table2-21](#) describes the fields in the **show vtp** command output.

Table2-21 show vtp Command Output Fields

Field	Description
Summary advertisements received	Total number of summary advertisements received.
Subset advertisements received	Total number of subset advertisements received.
Request advertisements received	Total number of request advertisements received.
Summary advertisements transmitted	Total number of summary advertisements transmitted.
Subset advertisements transmitted	Total number of subset advertisements transmitted.
Request advertisements transmitted	Total number of request advertisements transmitted.
Number of config revision errors	Number of config revision errors.
Number of config digest errors	Number of config revision digest errors.
Number of V1 summary errors	Number of V1 summary errors.
Trunk	Trunk port participating in VTP pruning.
Join Transmitted	Number of VTP-Pruning Joins transmitted.
Join Received	Number of VTP-Pruning Joins received.
Summary advts received from non-pruning-capable device	Number of Summary advertisements received from nonpruning-capable devices.
Number of existing VLANs	Total number of VLANs in the domain.
Configuration Revision	VTP revision number used to exchange VLAN information.
Maximum VLANs supported locally	Maximum number of VLANs allowed on the device.
Number of existing VLANs	Number of existing VLANs.
VTP Operating Mode	Indicates whether VTP is enabled or disabled.
VTP Domain Name	Name of the VTP domain.
VTP Pruning Mode	Indicates whether VTP pruning is enabled or disabled.
VTP V2 Mode	Indicates the VTP V2 mode as server, client, or transparent.
VTP Traps Generation	Indicates whether VTP trap generation mode is enabled or disabled.
MD5 digest	Checksum values.

Related Commands **vtp (global configuration mode)**
vtp client
vtp domain
vtp password
vtp pruning
vtp server
vtp transparent
vtp v2-mode

■ show vtp

snmp ifindex clear

To clear any previously configured **snmp ifindex** commands that were entered for a specific interface, use the **snmp ifindex clear** command.

snmp ifindex clear

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Interface configuration mode

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst4500 series switches.

Usage Guidelines Interface index persistence occurs when ifIndex values in the interface MIB (IF-MIB) persist across reboots and allow for consistent identification of specific interfaces using SNMP.

Use the **snmp ifindex clear** command on a specific interface when you want that interface to use the global configuration setting for ifIndex persistence. This command clears any ifIndex configuration commands previously entered for that specific interface.

Examples This example shows how to enable ifIndex persistence for all interfaces:

```
Router(config)# snmp-server ifindex persist
```

This example shows how to disable IfIndex persistence for FastEthernet 1/1 only:

```
Router(config)# interface fastethernet 1/1
Router(config-if)# no snmp ifindex persist
Router(config-if)# exit
```

This example shows how to clear the ifIndex configuration from the FastEthernet 1/1 configuration:

```
Router(config)# interface fastethernet 1/1
Router(config-if)# snmp ifindex clear
Router(config-if)# exit
```

As a result of this sequence of commands, ifIndex persistence is enabled for all interfaces that are specified by the **snmp-server ifindex persist** global configuration command.

Related Commands [snmp ifindex persist](#)
[snmp-server ifindex persist](#)

snmp ifindex persist

To enable ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) on a specific interface, use the **snmp ifindex persist** command. Use the **no** form of this command to disable ifIndex persistence only on a specific interface.

snmp ifindex persist

no snmp ifindex persist

Syntax Description This command has no arguments or keywords.

Defaults Disabled.

Command Modes Interface configuration mode

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst4500 series switches.

Usage Guidelines Interface index persistence occurs when ifIndex values in the IF-MIB persist across reboots and allow for consistent identification of specific interfaces using SNMP.

The **snmp ifindex persist** interface configuration command enables and disables ifIndex persistence for individual entries (that correspond to individual interfaces) in the ifIndex table of the IF-MIB.

The **snmp-server ifindex persist** global configuration command enables and disables ifIndex persistence for all interfaces on the routing device. This action applies only to interfaces that have ifDescr and ifIndex entries in the ifIndex table of the IF-MIB.

Examples This example shows how to enable ifIndex persistence for interface FastEthernet 1/1 only:

```
Router(config)# interface fastethernet 1/1
Router(config-if)# snmp ifindex persist
Router(config-if)# exit
```

This example shows how to enable ifIndex persistence for all interfaces, and then disable ifIndex persistence for interface FastEthernet 1/1 only:

```
Router(config)# snmp-server ifindex persist
Router(config)# interface fastethernet 1/1
Router(config-if)# no snmp ifindex persist
Router(config-if)# exit
```

Related Commands [snmp ifindex clear](#)
[snmp-server ifindex persist](#)

snmp-server enable traps

To enable SNMP notifications (traps or informs), use the **snmp-server enable traps** command. To disable all SNMP notifications, use the **no** form of this command.

snmp-server enable traps [**flash** [**insertion** | **removal**] | **fru-ctrl** | **port-security** [**trap-rate** *trap-rate*] | **removal** | **stp** | **vlancreate** | **vlandelete** | **vtp**]

no snmp-server enable traps **flash** [**insertion** | **removal**] | **fru-ctrl** | **port-security** [**trap-rate** *trap-rate*] | **removal** | **stp** | **vlancreate** | **vlandelete** | **vtp**]

Syntax Description		
flash	(Optional)	Controls the SNMP FLASH trap notifications.
insertion	(Optional)	Controls the SNMP Flash insertion trap notifications.
removal	(Optional)	Controls the SNMP Flash removal trap notifications.
fru-ctrl	(Optional)	Controls the SNMP entity FRU control trap notifications.
port-security	(Optional)	Controls the SNMP trap generation.
trap-rate <i>trap-rate</i>	(Optional)	Sets the number of traps per second.
stp	(Optional)	Controls all the traps defined in CISCO-STP-EXTENSIONS-MIB notifications.
vlancreate	(Optional)	Controls the SNMP VLAN created trap notifications.
vlandelete	(Optional)	Controls the SNMP VLAN deleted trap notifications.
vtp	(Optional)	Controls the SNMP VTP trap notifications.

Defaults SNMP notifications are disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines If you enter this command without an option, all notification types controlled by this command are enabled.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. To specify whether the notifications should be sent as traps or informs, use the **snmp-server host** [**traps** | **informs**] command.

The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send notifications, you must configure at least one **snmp-server host** command.

The following is a list of the MIBs used for the traps:

- **flash**—Controls SNMP FLASH traps from the CISCO-FLASH-MIB.
 - **insertion**—Controls the SNMP Flash insertion trap notifications.
 - **removal**—Controls the SNMP Flash removal trap notifications.
- **fru-ctrl**—Controls the FRU control traps from the CISCO-ENTITY-FRU-CONTROL-MIB.
- **port-security**—Controls the port-security traps from the CISCO-PORT-SECURITY-MIB.
- **stp**—Controls all the traps from the CISCO-STP-EXTENSIONS-MIB.
- **vlancreate**—Controls SNMP VLAN created trap notifications.
- **vlandelete**—Controls SNMP VLAN deleted trap notifications.
- **vtp**—Controls the VTP traps from the CISCO-VTP-MIB.

Examples

This example shows how to send all traps to the host specified by the name myhost.cisco.com, using the community string defined as public:

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
Switch(config)#
```

Related Commands

Refer to Cisco IOS documentation for additional **snmp-server enable traps** commands.

snmp-server ifindex persist

To globally enable ifIndex values that will remain constant across reboots for use by SNMP, use the **snmp-server ifindex persist** command. Use the **no** form of this command to globally disable ifIndex persistence.

snmp-server ifindex persist

no snmp-server ifindex persist

Syntax Description This command has no arguments or keywords.

Defaults Disabled.

Command Modes Global configuration mode

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst4500 series switches.

Usage Guidelines Interface index persistence occurs when ifIndex values in the IF-MIB persist across reboots and allow for consistent identification of specific interfaces using SNMP.

The **snmp-server ifindex persist** global configuration command does not override interface-specific configuration. To override the interface-specific configuration of ifIndex persistence, enter the **no snmp ifindex persist** and **snmp ifindex clear** interface configuration commands.

Entering the **no snmp-server ifindex persist** global configuration command enables and disables ifIndex persistence for all interfaces on the routing device using ifDescr and ifIndex entries in the ifIndex table of the IF-MIB.

Examples This example shows how to enable ifIndex persistence for all interfaces:

```
Router(config)# snmp-server ifindex persist
```

Related Commands [snmp ifindex clear](#)
[snmp ifindex persist](#)

snmp-server ifindex persist compress

To configure the format of the ifIndex table in compressed format, use the **snmp-server ifindex persist compress** command. Use the **no** form of this command to place the table in decompressed format.

snmp-server ifindex persist compress

no snmp-server ifindex persist compress

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration mode.

Command History	Release	Modification
	12.2(18)EW	Support for this command was introduced on the Catalyst4500 series switches.

Usage Guidelines This command is hidden on Supervisor Engine V and later supervisor engines because the ifIndex table is always in compressed format on those supervisor engines.

At bootup, if the nvram:ifIndex-table.gz file (the ifIndex table in compressed format) is present on a Supervisor Engine II+, Supervisor Engine III, or Supervisor Engine IV, the **snmp-server ifindex persist compress** command is automatically run even if the startup-config file does not have this configuration.

Examples This example shows how to enable compression of the ifIndex table:

```
Router(config)# snmp-server ifindex persist compress
```

This example shows how to disable compression of the ifIndex table:

```
Router(config)# no snmp-server ifindex persist compress
```

Related Commands

- [snmp ifindex clear](#)
- [snmp ifindex persist](#)
- [snmp-server ifindex persist](#)

spanning-tree backbonefast

To enable BackboneFast on a spanning tree VLAN, use the **spanning-tree backbonefast** command. To disable BackboneFast, use the **no** form of the command.

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(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines BackboneFast should be enabled on all Catalyst 4006 family switches to allow the detection of indirect link failures. Enabling BackboneFast starts the spanning tree reconfiguration more quickly.

Examples This example shows how to enable BackboneFast on all VLANs:

```
Switch(config)# spanning-tree backbonefast
Switch(config)#
```

Related Commands

- [spanning-tree cost](#)
- [spanning-tree port-priority](#)
- [spanning-tree portfast default](#)
- [spanning-tree portfast \(interface configuration mode\)](#)
- [spanning-tree uplinkfast](#)
- [spanning-tree vlan](#)
- [show spanning-tree](#)

spanning-tree bpdudfilter

To enable BPDU filtering on an interface, use the **spanning-tree bpdudfilter** command. To return to the default settings, use the **no** form of this command.

spanning-tree bpdudfilter { **enable** | **disable** }

no spanning-tree bpdudfilter

Syntax Description	enable	Enables BPDU filtering on this interface.
	disable	Disables BPDU filtering on this interface.
Defaults	Disabled	
Command Modes	Interface configuration	
Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines



Caution

Use care when entering the **spanning-tree bpdudfilter enable** command. Enabling BPDU filtering on an interface is approximately equivalent to disabling the spanning tree for this interface. It is possible to create bridging loops if this command is not correctly used.

When configuring Layer 2 protocol tunneling on all the service provider edge switches, you must enable spanning tree BPDU filtering on the 802.1Q tunnel ports by entering the **spanning-tree bpdudfilter enable** command.

BPDU filtering allows you to prevent a port from sending and receiving BPDUs. The configuration is applicable to the whole interface, whether it is trunking or not. This command has three states:

- **spanning-tree bpdudfilter enable**—This state unconditionally enables the BPDU filter feature on the interface.
- **spanning-tree bpdudfilter disable**—This state unconditionally disables the BPDU filter feature on the interface.
- **no spanning-tree bpdudfilter**—This state enables the BPDU filter feature on the interface if the interface is in operational PortFast state and if the **spanning-tree portfast bpdudfilter default** command is configured.

Examples

This example shows how to enable the BPDU filter feature on this interface:

```
Switch(config-if)# spanning-tree bpdudfilter enable
Switch(config-if)#
```

Related Commands

[show spanning-tree](#)
[spanning-tree portfast bpdudfilter default](#)

spanning-tree bpduguard

To enable BPDU guard on an interface, use the **spanning-tree bpduguard** command. To return to the default settings, use the **no** form of this command.

spanning-tree bpduguard { enable | disable }

no spanning-tree bpduguard

Syntax Description	enable	Enables BPDU guard on this interface.
	disable	Disables BPDU guard on this interface.

Defaults BPDU guard is disabled.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines BPDU guard is a feature that prevents a port from receiving BPDUs. This feature is typically used in a service provider environment where the administrator wants to prevent an access port from participating in the spanning tree. If the port still receives a BPDU, it is put in the ErrDisable state as a protective measure. This command has three states:

- **spanning-tree bpduguard enable**—This state unconditionally enables BPDU guard on the interface.
- **spanning-tree bpduguard disable**—This state unconditionally disables BPDU guard on the interface.
- **no spanning-tree bpduguard**—This state enables BPDU guard on the interface if it is in the operational PortFast state and if the **spanning-tree portfast bpduguard default** command is configured.

Examples This example shows how to enable BPDU guard on this interface:

```
Switch(config-if)# spanning-tree bpduguard enable
Switch(config-if)#
```

Related Commands [show spanning-tree](#)
[spanning-tree portfast bpduguard default](#)

spanning-tree cost

To calculate the path cost of STP on an interface, use the **spanning-tree cost** command. To revert to the default, use the **no** form of this command.

spanning-tree cost *cost*

no spanning-tree cost *cost*

Syntax Description

cost Path cost; valid values are from 1 to 200,000,000.

Defaults

The default settings are as follows:

- FastEthernet—19
- GigabitEthernet—1

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

When you configure the cost, higher values indicate higher costs. The range applies regardless of the protocol type specified. Path cost is calculated, based on interface bandwidth.

Examples

This example shows how to access an interface and set a path cost value of 250 for the spanning tree VLAN associated with that interface:

```
Switch(config)# interface fastethernet 2/1
Switch(config-if)# spanning-tree cost 250
Switch(config-if)#
```

Related Commands

[spanning-tree port-priority](#)
[spanning-tree portfast default](#)
[spanning-tree portfast \(interface configuration mode\)](#)
[spanning-tree uplinkfast](#)
[spanning-tree vlan](#)
[show spanning-tree](#)

spanning-tree etherchannel guard misconfig

To display an error message when a loop due to a channel misconfiguration is detected, use the **spanning-tree etherchannel guard misconfig** command. To disable the feature, use the **no** form of this command.

spanning-tree etherchannel guard misconfig

no spanning-tree etherchannel guard misconfig

Syntax Description This command has no arguments or keywords.

Defaults Spanning-tree EtherChannel guard is enabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines When an EtherChannel guard misconfiguration is detected, this error message is displayed:

```
%SPANTREE-2-CHNL_MISCFG:Detected loop due to etherchannel misconfig of interface
Port-Channel1
```

To determine which local ports are involved in the misconfiguration, enter the **show interfaces status err-disabled** command. To check the EtherChannel configuration on the remote device, enter the **show etherchannel summary** command on the remote device.

After you correct the configuration, enter the **shutdown** and the **no shutdown** commands on the associated port channel interface.

Examples This example shows how to enable the EtherChannel guard misconfiguration feature:

```
Switch(config)# spanning-tree etherchannel guard misconfig
Switch(config)#
```

Related Commands

- show interfaces status**
- show etherchannel**
- shutdown** (refer to Cisco IOS documentation)

spanning-tree extend system-id

To enable the extended system ID feature on a chassis that supports 1024 MAC addresses, use the **spanning-tree extend system-id** command. To disable the feature, use the **no** form of this command.

spanning-tree extend system-id

no spanning-tree extend system-id

Syntax Description This command has no arguments or keywords.

Defaults Enabled on systems that do not provide 1024 MAC addresses.

Command Modes Global configuration

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Releases 12.1(13)E and later support chassis with 64 or 1024 MAC addresses. For chassis with 64 MAC addresses, STP uses the extended system ID plus a MAC address to make the bridge ID unique for each VLAN.

You cannot disable the extended system ID on chassis that support 64 MAC addresses.

Enabling or disabling the extended system ID updates the bridge IDs of all active STP instances, which might change the spanning tree topology.

Examples This example shows how to enable the extended system ID:

```
Switch(config)# spanning-tree extend system-id
Switch(config)#
```

Related Commands [show spanning-tree](#)

spanning-tree guard

To enable root guard, use the **spanning-tree guard** command. To disable root guard, use the **no** form of this command.

spanning-tree guard {loop | root | none}

no spanning-tree guard

Syntax Description	Command	Description
	loop	Enables the loop guard mode on the interface.
	root	Enables root guard mode on the interface.
	none	Sets the guard mode to none.

Defaults Root guard is disabled.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Loop guard support was added.

Examples This example shows how to enable root guard:

```
Switch(config-if)# spanning-tree guard root
Switch(config-if)#
```

Related Commands [show spanning-tree](#)

spanning-tree link-type

To configure a link type for a port, use the **spanning-tree link-type** command. To return to the default settings, use the **no** form of this command.

spanning-tree link-type {point-to-point | shared}

no spanning-tree link-type

Syntax Description	point-to-point	Interface is a point-to-point link.
	shared	Interface is a shared medium.

Defaults Link type is derived from the duplex mode.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines RSTP+ fast transition only works on point-to-point links between two bridges.

By default, the switch derives the link type of a port from the duplex mode. A full-duplex port is considered as a point-to-point link while a half-duplex configuration is assumed to be on a shared link.

If you designate a port as a shared link, RSTP+ fast transition is forbidden, regardless of the duplex setting.

Examples This example shows how to configure the port as a shared link:

```
Switch(config-if)# spanning-tree link-type shared
Switch(config-if)#
```

Related Commands [show spanning-tree interface](#)

spanning-tree loopguard default

To enable loop guard as the default on all ports of a specific bridge, use the **spanning-tree loopguard default** command. To disable loop guard, use the **no** form of this command.

spanning-tree loopguard default

no spanning-tree loopguard default

Syntax Description This command has no keywords or arguments.

Defaults Loop guard is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Loop guard provides an additional security in the bridge network. Loop guard prevents alternate or root ports from becoming the designated port because of a failure leading to a unidirectional link.

Loop guard only operates on ports that are considered point-to-point by the spanning tree.

Individual loop-guard port configuration overrides this global default.

Examples This example shows how to enable loop guard:

```
Switch(config)# spanning-tree loopguard default
Switch(config)#
```

Related Commands

[show spanning-tree](#)
[spanning-tree guard](#)

spanning-tree mode

To switch between PVST+ and MST modes, use the **spanning-tree mode** command. To return to the default settings, use the **no** form of this command.

spanning-tree mode {pvst | mst | rapid-pvst}

no spanning-tree mode {pvst | mst | rapid-pvst}

Syntax Description	Command	Description
	pvst	Specifies PVST+ mode.
	mst	Specifies MST mode.
	rapid-pvst	Specifies Rapid PVST mode.

Defaults PVST+ mode

Command Modes Configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(19)EW	Support for the rapid-pvst keyword.

Usage Guidelines



Caution

Be careful when using the **spanning-tree mode** command to switch between PVST+ and MST modes. When you enter the command, all spanning tree instances are stopped for the previous mode and restarted in the new mode. Using this command may cause disruption of user traffic.

Examples

This example shows how to switch to MST mode:

```
Switch(config)# spanning-tree mode mst
Switch(config)#
```

This example shows how to return to the default mode (PVST):

```
Switch(config)# no spanning-tree mode
Switch(config)#
```

Related Commands [show spanning-tree mst](#)

spanning-tree mst

To set the path cost and port-priority parameters for any MST instance (including the CIST with instance ID0), use the **spanning-tree mst** command. To return to the default settings, use the **no** form of this command.

```
spanning-tree mst instance-id [cost cost] | [port-priority prio]
```

```
no spanning-tree mst instance-id {cost | port-priority}
```

Syntax Description

<i>instance-id</i>	Instance ID number; valid values are from 0 to 15.
cost <i>cost</i>	(Optional) Specifies the path cost for an instance; valid values are from 1 to 200000000.
port-priority <i>prio</i>	(Optional) Specifies the port priority for an instance; valid values are from 0 to 240 in increments of 16.

Defaults

Port priority is **128**.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Higher **cost** *cost* values indicate higher costs. When entering the *cost* value, do not include a comma in the entry; for example, enter **1000**, not **1,000**.

Higher **port-priority** *prio* values indicate smaller priorities.

By default, cost depends on the port speed; faster interface speeds indicate smaller costs. MST always uses long path costs.

Examples

This example shows how to set the interface path cost:

```
Switch(config-if)# spanning-tree mst 0 cost 17031970
Switch(config-if)#
```

This example shows how to set the interface priority:

```
Switch(config-if)# spanning-tree mst 0 port-priority 64
Switch(config-if)#
```

Related Commands

[show spanning-tree mst](#)
[spanning-tree port-priority](#)

spanning-tree mst configuration

To enter the MST configuration submode, use the **spanning-tree mst configuration** command. To return to the default MST configuration, use the **no** form of this command.

spanning-tree mst configuration

no spanning-tree mst configuration

Syntax Description This command has no arguments or keywords.

Defaults The default settings are as follows:

- No VLANs are mapped to any MST instance.
- All VLANs are mapped to the CIST instance.
- The region name is an empty string.
- The revision number is 0.

Command Modes Global configuration

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines The MST configuration consists of three main parameters:

- Instance VLAN mapping (see the **instance** command)
- Region name (see the **name** command)
- Configuration revision number (see the **revision** command)

By default, the value for the MST configuration is the default value for all its parameters.

The **abort** and **exit** commands allow you to exit the MST configuration submode. The difference between the two commands depends on whether you want to save your changes or not.

The **exit** command commits all the changes before leaving MST configuration submode. If you do not map secondary VLANs to the same instance as the associated primary VLAN, when you exit the MST configuration submode, a warning message displays and lists the secondary VLANs that are not mapped to the same instance as the associated primary VLAN. The warning message is as follows:

```
These secondary vlans are not mapped to the same instance as their primary:
->3
```

The **abort** command leaves the MST configuration submode without committing any changes.

Whenever you change an MST configuration submode parameter, it can cause a loss of connectivity. To reduce the number of service disruptions, when you enter the MST configuration submode, you are changing a copy of the current MST configuration. When you are done editing the configuration, you can apply all the changes at once by using the **exit** keyword, or you can exit the submode without committing any change to the configuration by using the **abort** keyword.

In the unlikely event that two users enter a new configuration at exactly at the same time, this warning message is displayed:

```
Switch(config-mst)# exit
% MST CFG:Configuration change lost because of concurrent access
Switch(config-mst)#
```

Examples

This example shows how to enter the MST configuration submode:

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)#
```

This example shows how to reset the MST configuration to the default settings:

```
Switch(config)# no spanning-tree mst configuration
Switch(config)#
```

Related Commands

[instance](#)
[name](#)
[revision](#)
[show spanning-tree mst](#)

spanning-tree mst forward-time

To set the forward delay timer for all the instances, use the **spanning-tree mst forward-time** command. To return to the default settings, use the **no** form of the command.

spanning-tree mst forward-time *seconds*

no spanning-tree mst forward-time

Syntax Description	<i>seconds</i>	Number of seconds to set the forward delay timer for all the instances on the Catalyst4500 series switch; valid values are from 4 to 30 seconds.
Defaults	The forward delay timer is set for 15 seconds.	
Command Modes	Global configuration	
Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Examples	This example shows how to set the forward-delay timer: <pre>Switch(config)# spanning-tree mst forward-time 20 Switch(config)#</pre>	
Related Commands	show spanning-tree mst	

spanning-tree mst hello-time

To set the hello-time delay timer for all the instances, use the **spanning-tree mst hello-time** command. To return to the default settings, use the **no** form of the command.

spanning-tree mst hello-time *seconds*

no spanning-tree mst hello-time

Syntax Description	<i>seconds</i>	Number of seconds to set the hello-time delay timer for all the instances on the Catalyst4500 series switch; valid values are from 1 to 10 seconds.
Defaults	The hello-time delay timer is set for 2 seconds.	
Command Modes	Global configuration	
Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Usage Guidelines	If you do not specify the <i>hello-time</i> value, the value is calculated from the network diameter.	
Examples	This example shows how to set the hello-time delay timer: <pre>Switch(config)# spanning-tree mst hello-time 3 Switch(config)#</pre>	
Related Commands	show spanning-tree mst	

spanning-tree mst max-age

To set the max-age timer for all the instances, use the **spanning-tree mst max-age** command. To return to the default settings, use the **no** form of the command.

spanning-tree mst max-age *seconds*

no spanning-tree mst max-age

Syntax Description	<i>seconds</i>	Number of seconds to set the max-age timer for all the instances on the Catalyst4500 series switch; valid values are from 6 to 40 seconds.
Defaults	The max-age timer is set for 20 seconds.	
Command Modes	Global configuration	
Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Examples	This example shows how to set the max-age timer: <pre>Switch(config)# spanning-tree mst max-age 40 Switch(config)#</pre>	
Related Commands	show spanning-tree mst	

spanning-tree mst max-hops

To specify the number of possible hops in the region before a BPDU is discarded, use the **spanning-tree mst max-hops** command. To return to the default settings, use the **no** form of the command.

spanning-tree mst max-hops *hopnumber*

no spanning-tree mst max-hops

Syntax Description	<i>hopnumber</i> Number of possible hops in the region before a BPDU is discarded; valid values are from 1 to 40 hops.				
Defaults	Number of hops is 20.				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(12c)EW</td> <td>Support for this command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Release	Modification				
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.				
Examples	<p>This example shows how to set the number of possible hops in the region before a BPDU is discarded to 25:</p> <pre>Switch(config)# spanning-tree mst max-hops 25 Switch(config)#</pre>				
Related Commands	show spanning-tree mst				

spanning-tree mst root

To designate the primary root, secondary root, bridge priority, and timer value for an instance, use the **spanning-tree mst root** command. To return to the default settings, use the **no** form of the command.

```
spanning-tree mst instance-id root {primary | secondary} | {priority prio} [diameter dia
[hello-time hello]]
```

```
no spanning-tree mst root
```

Syntax Description

<i>instance-id</i>	Instance identification number; valid values are from 1 to 15.
root	Configures switch as the root switch.
primary	Sets a high enough priority (low value) to make the bridge root of the spanning-tree instance.
secondary	Designates this switch as a secondary root, if the primary root fails.
priority <i>prio</i>	Sets the bridge priority; see the “Usage Guidelines” section for valid values and additional information.
diameter <i>dia</i>	(Optional) Sets the timer values for the bridge based on the network diameter; valid values are from 2 to 7.
hello-time <i>hello</i>	(Optional) Specifies the duration between the generation of configuration messages by the root switch.

Defaults

Bridge priority is 32768.

Command Modes

Global configuration

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The bridge priority can be set in increments of 4096 only. When you set the priority, valid values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.

You can set the priority to 0 to make the switch root.

The **spanning-tree root secondary** bridge priority value is 16384.

The **diameter** *dia* and **hello-time** *hello* options are available for instance 0 only.

If you do not specify the *hello_time* value, the value is calculated from the network diameter.

Examples

This example shows how to set the bridge priority:

```
Switch(config)# spanning-tree mst 0 root priority 4096
Switch(config)#
```

This example shows how to set the priority and timer values for the bridge:

```
Switch(config)# spanning-tree mst 0 root primary diameter 7 hello-time 2
Switch(config)# spanning-tree mst 5 root primary
Switch(config)#
```

Related Commands [show spanning-tree mst](#)

spanning-tree pathcost method

To set the path cost calculation method, use the **spanning-tree pathcost method** command. To revert to the default setting, use the **no** form of this command.

spanning-tree pathcost method { long | short }

no spanning-tree pathcost method

Syntax Description	long	Specifies 32-bit-based values for port path costs.
	short	Specifies 16-bit-based values for port path costs.

Defaults Port path cost has 32-bit-based values.

Command Modes Global configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines This command applies to all the spanning tree instances on the switch.

The **long** path cost calculation method uses all the 32 bits for path cost calculation and yields values in the range of 1 through 200,000,000.

The **short** path cost calculation method (16 bits) yields values in the range of 1 through 65,535.

Examples This example shows how to set the path cost calculation method to long:

```
Switch(config# ) spanning-tree pathcost method long
Switch(config# )
```

This example shows how to set the path cost calculation method to short:

```
Switch(config# ) spanning-tree pathcost method short
Switch(config# )
```

Related Commands [show spanning-tree](#)

spanning-tree portfast (interface configuration mode)

To enable PortFast mode, where the interface is immediately put into the forwarding state upon linkup without waiting for the timer to expire, use the **spanning-tree portfast** command. To return to the default setting, use the **no** form of this command.

spanning-tree portfast {disable | trunk}

no spanning-tree portfast

Syntax Description	disable	Disables PortFast on the interface.
	trunk	Enables PortFast on the interface even while in the trunk mode.

Defaults PortFast mode is disabled.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	The disable and trunk options were added.

Usage Guidelines You should use this feature only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt the Catalyst4500 series switch and network operation.

An interface with PortFast mode enabled is moved directly to the spanning tree forwarding state when linkup occurs without waiting for the standard forward-time delay.

Be careful when using the **no spanning-tree portfast** command. This command does not disable PortFast if the **spanning-tree portfast default** command is enabled.

This command has four states:

- **spanning-tree portfast**—This command enables PortFast unconditionally on the given port.
- **spanning-tree portfast disable**—This command explicitly disables PortFast for the given port. The configuration line shows up in the running-configuration as it is not the default.
- **spanning-tree portfast trunk**—This command allows you to configure PortFast on trunk ports.



Note If you enter the **spanning-tree portfast trunk** command, the port is configured for PortFast even when in the access mode.

- **no spanning-tree portfast**—This command implicitly enables PortFast if the **spanning-tree portfast default** command is defined in global configuration and if the port is not a trunk port. If you do not configure PortFast globally, the **no spanning-tree portfast** command is equivalent to the **spanning-tree portfast disable** command.

Examples

This example shows how to enable PortFast mode:

```
Switch(config-if)# spanning-tree portfast
Switch(config-if)
```

Related Commands

[spanning-tree cost](#)
[spanning-tree port-priority](#)
[spanning-tree portfast default](#)
[spanning-tree uplinkfast](#)
[spanning-tree vlan](#)
[show spanning-tree](#)

spanning-tree portfast bpdudfilter default

To enable the BPDU filtering by default on all PortFast ports, use the **spanning-tree portfast bpdudfilter default** command. To return to the default settings, use the **no** form of this command.

spanning-tree portfast bpdudfilter default

no spanning-tree portfast bpdudfilter default

Syntax Description This command has no keywords or arguments.

Defaults BPDU filtering is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines The **spanning-tree portfast bpdudfilter default** command enables BPDU filtering globally on the Catalyst4500 series switch. BPDU filtering prevents a port from sending or receiving any BPDUs. You can override the effects of the **spanning-tree portfast bpdudfilter default** command by configuring BPDU filtering at the interface level.



Note

Be careful when enabling BPDU filtering. Functionality is different when enabling on a per-port basis or globally. When enabled globally, BPDU filtering is applied only on ports that are in an operational PortFast state. Ports still send a few BPDUs at linkup before they effectively filter outbound BPDUs. If a BPDU is received on an edge port, it immediately loses its operational PortFast status and BPDU filtering is disabled.

When enabled locally on a port, BPDU filtering prevents the Catalyst4500 series switch from receiving or sending BPDUs on this port.



Caution

Be careful when using this command. This command can cause bridging loops if not used correctly.

Examples This example shows how to enable BPDU filtering by default:

```
Switch(config)# spanning-tree portfast bpdudfilter default
Switch(config)#
```

Related Commands

[show spanning-tree mst](#)
[spanning-tree bpdupfilter](#)

spanning-tree portfast bpduguard default

To enable the BPDU guard feature by default on all PortFast ports, use the **spanning-tree portfast bpduguard default** command. To return to the default settings, use the **no** form of this command.

spanning-tree portfast bpduguard default

no spanning-tree portfast bpduguard default

Syntax Description This command has no keywords or arguments.

Defaults BPDU guard is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines



Caution

Be careful when using this command. You should use this command only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt the Catalyst4500 series switch and network operation.

BPDU guard disables a port if it receives a BPDU. BPDU guard is applied only on ports that are PortFast enabled and are in an operational PortFast state.

Examples

This example shows how to enable BPDU guard by default:

```
Switch(config)# spanning-tree portfast bpduguard default
Switch(config)#
```

Related Commands

[show spanning-tree mst](#)
[spanning-tree bpduguard](#)

spanning-tree portfast default

To globally enable PortFast by default on all access ports, use the **spanning-tree portfast default** command. To disable PortFast as default on all access ports, use the **no** form of this command.

spanning-tree portfast default

no spanning-tree portfast default

Syntax Description This command has no arguments or keywords.

Defaults PortFast is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines



Caution

Be careful when using this command. You should use this command only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt the Catalyst4500 series switch and network operation.

An interface with PortFast mode enabled is moved directly to the spanning tree forwarding state when linkup occurs without waiting for the standard forward-time delay.

You can enable PortFast mode on individual interfaces using the **spanning-tree portfast (interface configuration mode)** command.

Examples This example shows how to globally enable PortFast by default on all access ports:

```
Switch(config)# spanning-tree portfast default
Switch(config)#
```

Related Commands [show spanning-tree](#)
[spanning-tree portfast \(interface configuration mode\)](#)

spanning-tree port-priority

To prioritize an interface when two bridges compete for position as the root bridge, use the **spanning-tree port-priority** command. The priority you set breaks the tie. To revert to the default setting, use the **no** form of this command.

spanning-tree port-priority *port_priority*

no spanning-tree port-priority

Syntax Description

port_priority Port priority; valid values are from 0 to 240 in increments of 16.

Defaults

Port priority value is set to 128.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

This example shows how to increase the possibility that the spanning tree instance 20 will be chosen as the root-bridge on interface FastEthernet 2/1:

```
Switch(config-if)# spanning-tree port-priority 0
Switch(config-if)#
```

Related Commands

[spanning-tree cost](#)
[spanning-tree portfast default](#)
[spanning-tree portfast \(interface configuration mode\)](#)
[spanning-tree uplinkfast](#)
[spanning-tree vlan](#)
[show spanning-tree](#)

spanning-tree uplinkfast

To enable the UplinkFast feature, use the **spanning-tree uplinkfast** command. To disable UplinkFast, use the **no** form of the command.

spanning-tree uplinkfast [**max-update-rate** *packets-per-second*]

no spanning-tree uplinkfast [**max-update-rate**]

Syntax Description	max-update-rate (Optional) Specifies the maximum rate (in packets per second) at which update packets are sent; valid values are from 0 to 65535. <i>packets_per_second</i>
---------------------------	---

Defaults	The default settings are as follows: <ul style="list-style-type: none"> • Disabled. • Maximum update rate is 150.
-----------------	---

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

Command History	<table border="1"> <thead> <tr> <th style="border: none;">Release</th> <th style="border: none;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border: none;">12.1(8a)EW</td> <td style="border: none;">Support for this command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Release	Modification				
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.				

Usage Guidelines	<p>This command should be used only on access switches.</p> <p>When UplinkFast is configured, the bridge priority is changed to 49,152 so that this switch will not be selected as root. All interface path costs of all spanning tree interfaces belonging to the specified spanning tree instances are also increased by 3000.</p> <p>When spanning tree detects that the root interface has failed, the UplinkFast feature causes an immediate switchover to an alternate root interface, transitioning the new root interface directly to the forwarding state. During this time, a topology change notification is sent. To minimize the disruption caused by the topology change, a multicast packet is sent to 01-00-0C-CD-CD-CD for each station address in the forwarding bridge except for those associated with the old root interface.</p> <p>Use the spanning-tree uplinkfast max-update-rate command to enable UplinkFast (if not already enabled) and change the rate at which update packets are sent. Use the no form of the command to return the default rate of 150 packets per second.</p>
-------------------------	---

Examples	<p>This example shows how to enable UplinkFast and set the maximum rate to 200 packets per second:</p> <pre>Switch(config)# spanning-tree uplinkfast Switch(config)# spanning-tree uplinkfast max-update-rate 200</pre>
-----------------	---

■ spanning-tree uplinkfast

Related Commands

[spanning-tree cost](#)
[spanning-tree port-priority](#)
[spanning-tree portfast default](#)
[spanning-tree portfast \(interface configuration mode\)](#)
[spanning-tree vlan](#)

spanning-tree vlan

To configure STP on a per-VLAN basis, use the **spanning-tree vlan** command. To return to the default value, use the **no** form of this command.

```
spanning-tree vlan vlan_id [forward-time seconds | hello-time seconds | max-age seconds |
priority priority | protocol protocol | 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 identification number; valid values are from 1 to 4094.
forward-time <i>seconds</i>	(Optional) Sets the STP forward delay time; valid values are from 4 to 30 seconds.
hello-time <i>seconds</i>	(Optional) Specifies, in seconds, the time between configuration messages generated by the root switch; valid values are from 1 to 10 seconds.
max-age <i>seconds</i>	(Optional) Sets the maximum time, in seconds, that the information in a BPDU is valid; valid values are from 6 to 40 seconds.
priority <i>priority</i>	(Optional) Sets the STP bridge priority; valid values are from 0 to 65535.
protocol <i>protocol</i>	(Optional) Specifies the protocol.
root primary	(Optional) Forces this switch to be the root bridge.
root secondary	(Optional) Specifies this switch act as the root switch should the primary root fail.
diameter <i>net-diameter</i>	(Optional) Specifies the maximum number of bridges between two end stations; valid values are from 2 to 7.

Defaults

The default settings are as follows:

- Forward-time—15 seconds
- Hello-time—2 seconds
- Max-age—20 seconds
- Priority—32768 with STP enabled; 128 with MST enabled
- Root—No STP root

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Support for extended addressing was added.

Usage Guidelines

When you are setting the **max-age seconds** value, if a bridge does not hear BPDUs from the root bridge within the specified interval, it assumes that the network has changed and recomputes the spanning tree topology.

The **spanning-tree root primary** command alters the switch bridge priority to 8192. If you enter the **spanning-tree root primary** command and the switch does not become root, then the bridge priority is changed to 100 less than the bridge priority of the current bridge. If the switch does not become root, an error will result.

The **spanning-tree root secondary** command alters the switch bridge priority to 16384. If the root switch fails, this switch becomes the next root switch.

Use the **spanning-tree root** commands on backbone switches only.

Examples

This example shows how to enable spanning tree on VLAN 200:

```
Switch(config)# spanning-tree vlan 200
Switch(config)#
```

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
Switch(config)#
```

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
Switch(config)#
```

Related Commands

[spanning-tree cost](#)
[spanning-tree port-priority](#)
[spanning-tree portfast default](#)
[spanning-tree portfast \(interface configuration mode\)](#)
[spanning-tree uplinkfast](#)
[show spanning-tree](#)

speed

To configure the interface speed, use the **speed** command. To disable a speed setting, use the **no** form of this command.

speed [10 | 100 | 1000 | auto | nonegotiate]

no speed

Syntax Description		
10	(Optional)	Configures the interface to transmit at 10 Mbps.
100	(Optional)	Configures the interface to transmit at 100 Mbps.
1000	(Optional)	Configures the interface to transmit at 1000 Mbps.
auto	(Optional)	Enables the interface to auto-negotiate the speed.
nonegotiate	(Optional)	Enables the interface to not negotiate the speed.

Defaults

The default values are shown in the following table:

Interface Type	Supported Syntax	Default Setting
10/100-Mbps module	speed [10 100 auto]	Auto
100-Mbps fiber modules	Not applicable	Not applicable
Gigabit Ethernet Interface	speed nonegotiate	Nonegotiate
10/100/1000	speed [10 100 1000 auto]	Auto
1000	Not applicable	Not applicable

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

[Table2-22](#) lists the supported command options by interface.

Table2-22 Supported speed Command Options

Interface Type	Supported Syntax	Default Setting	Guidelines
10/100-Mbps module	speed [10 100 auto]	auto	If the speed is set to auto, you will not be able to set duplex. If the speed is set to 10 or 100 and you do not configure the duplex setting, the duplex is set to half.
100-Mbps fiber modules	Not applicable.	Not applicable.	Not applicable.
Gigabit Ethernet Interface	speed nonegotiate	Nonegotiate is enabled.	This is only applicable to Gigabit Ethernet ports.
10/100/1000	speed [10 100 1000 auto]	auto	If the speed is set to auto or 1000, you will not be able to set duplex. If the speed is set to 10 or 100 and you do not configure the duplex setting, the duplex is set to half.
1000	Not applicable.	Not applicable.	The speed is always 1000. The duplex is half.

If you configure the interface speed and duplex commands manually and enter a value other than **speed auto** (for example, 10 or 100 Mbps), be sure that you configure the connecting interface speed command to a matching speed but do not use the auto parameter.

When manually configuring the interface speed to either 10 or 100 Mbps, the switch prompts you to also configure duplex mode on the interface.

**Note**

Catalyst 4006 switches cannot automatically negotiate interface speed and duplex mode if either connecting interface is configured to a value other than **auto**.

**Caution**

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

[Table2-23](#) describes the system's performance for different combinations of the duplex and speed modes. The specified **duplex** command configured with the specified **speed** command produces the resulting system action.

Table2-23 System Action Using duplex and speed Commands

duplex Command	speed Command	Resulting System Action
duplex half or duplex full	speed auto	Autonegotiates both speed and duplex modes
duplex half	speed 10	Forces 10 Mbps and half duplex
duplex full	speed 10	Forces 10 Mbps and full duplex
duplex half	speed 100	Forces 100 Mbps and half duplex

Table2-23 System Action Using duplex and speed Commands (continued)

duplex Command	speed Command	Resulting System Action
duplex full	speed 100	Forces 100 Mbps and full duplex
duplex full	speed 1000	Forces 1000 Mbps and full duplex

This example shows how to configure the interface to transmit at 100 Mbps:

```
Switch(config-if)# speed 100
Switch(config-if)#
```

Related Commands**duplex**

interface (refer to Cisco IOS documentation)

show controllers (refer to Cisco IOS documentation)

show interfaces (refer to Cisco IOS documentation)

storm-control

To enable broadcast storm control on a port, and to specify what to do when a storm occurs on a port, use the **storm-control** interface configuration command. Use the **no** form of this command to disable storm control for broadcast traffic and disable the specified storm-control action.

storm-control {**broadcast level** *high level* [*lower level*]} | **action** {**shutdown** | **trap**}}

no storm-control {**broadcast level** *level* [*lower level*]} | **action** {**shutdown** | **trap**}}

Syntax Description		
broadcast		Enables broadcast storm control on the port.
level <i>high-level lower-level</i>		Defines the rising and falling suppression levels: <ul style="list-style-type: none"> <i>high-level</i>—Rising suppression level as a percent of total bandwidth, up to two decimal places; valid values are from 0 to 100 percent. Blocks the flooding of storm packets when the value specified for <i>level</i> is reached. <i>lower-level</i>—(Optional) Falling suppression level as a percent of total bandwidth, up to two decimal places; valid values are from 0 to 100. This value must be less than the rising suppression value.
action		Directs the switch to take action when a storm occurs on a port.
shutdown		Disables the port during a storm.
trap		Sends an SNMP trap when a storm occurs. This keyword is available but not supported in 12.1(19)EW.

Defaults Broadcast storm control is disabled. All packets are passed.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Enter the **storm-control broadcast level** command to enable traffic storm control on the interface, configure the traffic storm control level, and apply the traffic storm control level to broadcast traffic on the interface.

The Catalyst4500 series switch supports broadcast traffic storm control on all LAN ports.

The period is required when you enter the fractional suppression level.

The suppression level is entered as a percentage of the total bandwidth. A threshold value of 100 percent indicates that no limit is placed on traffic. A value of 0.0 means that all specified traffic on that port is blocked.

Enter the **show interfaces counters storm-control** command to display the discard count.

Enter the **show running-config** command to display the enabled suppression mode and level setting.

To turn off suppression for the specified traffic type, you can do one of the following:

- Set the *high-level* value to 100 percent for the specified traffic type.
- Use the **no** form of this command.

Lower level is ignored for interfaces that perform storm control in hardware.

Examples

This example shows how to enable broadcast storm control on a port with a 75.67 percent rising suppression level:

```
Switch(config-if)# storm-control broadcast level 75.67
```

This example shows how to disable the port during a storm:

```
Switch(config-if)# storm-control action shutdown
```

This example shows how to disable storm control on a port:

```
Switch(config-if)# no storm-control broadcast level
```

This example shows how to disable storm control by setting high level to 200 percent:

```
Switch(config-if)# storm-control broadcast level 200
```

Related Commands

[show interfaces counters](#)
[show running-config](#)

storm-control broadcast include multicast

To enable multicast storm control on a port, use the **storm-control broadcast include multicast** command. Use the **no** form of this command to disable multicast storm control.

storm-control broadcast include multicast

no storm-control broadcast include multicast

Syntax Description This command has no arguments or keywords.

Defaults Multicast storm control is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines This command prompts the hardware to filter multicast packets if it is already filtering broadcast packets.

Examples This example shows how to enable multicast storm control globally:

```
Switch(config)# storm-control broadcast include multicast
Switch(config)#
```

Related Commands [storm-control](#)

switchport

To modify the switching characteristics of a Layer 2 switch interface, use the **switchport** command. To return the interface to the routed-interface status and cause all further Layer 2 configuration to be erased, use the **no** form of this command without parameters.

```
switchport [access vlan vlan_num] | [nonegotiate] | [voice vlan {vlan_id | dot1p | none | untagged}]
```

```
no switchport [access | nonegotiate | voice vlan]
```

Syntax Description	
access vlan <i>vlan_num</i>	(Optional) Sets the VLAN when the interface is in access mode; valid values are from 1 to 1005.
nonegotiate	(Optional) Specifies DISL/DTP negotiation packets will not be sent on the interface.
voice vlan <i>vlan_id</i>	(Optional) Specifies number of the VLAN; valid values are from 1 to 1005.
dot1p	(Optional) Specifies PVID packets tagged as priority.
none	(Optional) Specifies that the telephone and voice VLAN do not communicate.
untagged	(Optional) Specifies untagged PVID packets.

Defaults

The default settings are as follows:

- Switchport trunking mode is enabled.
- Dynamic negotiation parameter is set to auto.
- Access VLANs and trunk interface native VLANs are a default VLAN corresponding to the platform or interface hardware.
- All VLAN lists include all VLANs.
- No voice VLAN is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(11)EW	Support for voice VLAN was added.

Usage Guidelines

The **no switchport** command shuts the port down and then re-enables it, which may generate messages on the device to which the port is connected.

The **no** form of the **switchport access** command resets the access mode VLAN to the appropriate default VLAN for the device. The **no** form of the **switchport nonegotiate** command removes **nonegotiate** status.

When you are using the **nonegotiate** keyword, DISL/DTP negotiation packets will not be sent on the interface. The device will trunk or not trunk according to the **mode** parameter given: **access** or **trunk**. This command will return an error if you attempt to execute it in **dynamic (auto or desirable)** mode.

The voice VLAN is automatically set to VLAN 1 unless you use one of the optional keywords.

If you use the **switch port voice vlan** command for an interface, the interface cannot join a port channel.

When you use the **switchport voice vlan** command the output for the **show running-config** command changes to show the voice VLAN set.

Examples

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
Switch(config-if)#
```

This example shows how to cause a port interface in access mode, configured as a switched interface, to operate in VLAN 2:

```
Switch(config-if)# switchport access vlan 2
Switch(config-if)#
```

This example shows how to cause a port interface, configured as a switched interface, to refrain from negotiating trunking mode and act as a trunk or access port (depending on the **mode** set):

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

This example shows how to set the voice VLAN for the interface to VLAN 2:

```
Switch(config-if)# switchport voice vlan 2
switchport voice vlan 2
Switch(config-if)#
```

Related Commands

[show interfaces switchport](#)

switchport access vlan

To set the VLAN when an interface is in access mode, use the **switchport access vlan** command. To reset the access mode VLAN to the appropriate default VLAN for the device, use the **no** form of this command.

```
switchport access [vlan {vlan-id | dynamic}]
```

```
no switchport access vlan
```

Syntax Description

<i>vlan-id</i>	(Optional) Number of the VLAN on the interface in access mode; valid values are from 1 to 4094.
dynamic	(Optional) Enables VMPS control of the VLAN.

Defaults

The default settings are as follows:

- Access VLAN and trunk interface native VLAN are default VLANs corresponding to the platform or interface hardware.
- All VLAN lists include all VLANs.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(13)EW	Support for VPMS was added.

Usage Guidelines

You must enter the **switchport** command without any keywords to configure the LAN interface as a Layer 2 interface before you can enter the **switchport access vlan** command. This action is required only if you have not already entered the **switchport** command for the interface.

Entering the **no switchport** command shuts the port down and then reenables it, which could generate messages on the device to which the port is connected.

The **no** form of the **switchport access vlan** command resets the access mode VLAN to the appropriate default VLAN for the device.

If your system is configured with a Supervisor Engine 1, valid values for *vlan-id* are from 1 to 1005. If your system is configured with a Supervisor Engine 2, valid values for *vlan-id* are from 1 to 4094. Extended-range VLANs are not supported on systems configured with a Supervisor Engine 1.

Examples

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
Switch(config-if)#
```

**Note**

This command 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.

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  
Switch(config-if)#
```

Related Commands[show interfaces switchport](#)

switchport block

To prevent unknown multicast or unicast packets from being forwarded, use the **switchport block** interface configuration command. 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	Specifies that unknown multicast traffic should be blocked.
unicast	Specifies that unknown unicast traffic should be blocked.

Defaults

Unknown multicast and unicast traffic are not blocked.

All traffic with unknown MAC addresses is sent to all ports.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

You can block unknown multicast or unicast traffic on switch ports.

Blocking unknown multicast or unicast traffic is not automatically enabled on switch ports; you must explicitly configure it.



Note

For more information about blocking packets, refer to 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

[show interfaces switchport](#)

switchport mode

To set the interface type, use the **switchport mode** command. To reset the mode to the appropriate default mode for the device, use the **no** form of the command.

switchport mode { **access** | **dot1q-tunnel** | **trunk** | **dynamic** { **auto** | **desirable** } }

switchport mode private-vlan { **host** | **promiscuous** | **trunk** }

no switchport mode dot1q-tunnel

no switchport mode private-vlan

Syntax Description		
access		Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
dot1q-tunnel		Specifies an 802.1Q tunnel port.
trunk		Specifies a trunking VLAN Layer 2 interface.
dynamic auto		Specifies that the interface convert the link to a trunk link.
dynamic desirable		Specifies that the interface actively attempt to convert the link to a trunk link.
private-vlan host		Specifies that the ports with a valid PVLAN trunk association becomes active host private VLAN trunk ports.
private-vlan promiscuous		Specifies that the ports with a valid PVLAN mapping become active promiscuous ports.
private-vlan trunk		Specifies that the ports with a valid PVLAN trunk association becomes active host private VLAN trunk ports.

Defaults

Link converts to a trunk link.
dot1q tunnel ports are disabled.

Command Modes

Interface configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(18)EW	Support was added for configuring dot1q tunnel ports.

Usage Guidelines

If you enter **access** mode, the interface goes into permanent nontrunking mode and negotiates to convert the link into a nontrunk link even if the neighboring interface does not approve the change.

If you enter **trunk** mode, the interface goes into permanent trunking mode and negotiates to convert the link into a trunk link even if the neighboring interface does not approve the change.

If 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.

If you enter **dynamic desirable** mode, the interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode.

If you enter specify the **dot1q-tunnel** keyword, the port is set unconditionally as an 802.1Q tunnel port.

The port becomes inactive if you configure it as a private VLAN trunk port and one of the following applies:

- Port does not have a valid PVLAN association.
- Port does not have valid allowed normal VLANs.

If a private port PVLAN association or mapping is deleted, or if a private port is configured as a SPAN destination, it becomes inactive.

Examples

This example shows how to set the interface to dynamic desirable mode:

```
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)#
```

This example shows how to set a port to PVLAN host mode:

```
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)#
```

This example shows how to set a port to private VLAN trunk:

```
Switch(config-if)# switchport mode private-vlan trunk
Switch(config-if)#
```

This example shows how to configure a port for an 802.1Q tunnel port:

```
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)#
```

You can verify your settings by entering the **show interfaces switchport** command and examining information in the Administrative Mode and Operational Mode rows.

Related Commands

[show interfaces switchport](#)
[switchport](#)
[switchport private-vlan host-association](#)
[switchport private-vlan mapping](#)

switchport port-security

To enable port security on an interface, use the **switchport port-security** command. To disable port security and set parameters to their default states, use the **no** form of this command.

```
switchport port-security [aging {static | time time | type {absolute | inactivity}}] |
limit rate invalid-source-mac [N | none] | mac-address mac-address | mac-address sticky
[mac-address] | maximum value | violation {restrict | shutdown}}
```

```
no switchport port-security [aging {static | time time | type {absolute | inactivity}}] |
limit rate invalid-source-mac [N | none] | mac-address mac-address | mac-address sticky
[mac-address] | maximum value | violation {restrict | shutdown}}
```

Syntax Description	
aging	(Optional) Specifies aging for port security.
static	(Optional) Enables aging for statically configured secure addresses on this port.
time <i>time</i>	(Optional) Specifies the aging time for this port. The valid values are from 0 to 1440 minutes. If the time is 0, aging is disabled for this port.
type absolute	(Optional) Sets the aging type as absolute aging. All the secure addresses on this port age out exactly after the time (minutes) specified and are removed from the secure address list.
type inactivity	(Optional) Sets the aging type as inactivity aging. 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.
limit rate invalid-source-mac	(Optional) Sets the rate limit for bad packets. This rate limit also applies to the port where DHCP snooping security mode is enabled as filtering the IP and MAC address.
N none	(Optional) Supplies a rate limit (N) or indicates none (none).
mac-address <i>mac-address</i>	(Optional) Specifies a secure MAC address for the interface; a 48-bit MAC address. You can add additional secure MAC addresses up to the maximum value that is configured.
sticky	(Optional) Configures dynamic addresses as sticky on the interface.
maximum <i>value</i>	(Optional) Sets the maximum number of secure MAC addresses for the interface. Valid values are from 1 to 1024. The default setting is 1.
violation	(Optional) Sets the security violation mode and action to be taken if port security is violated.
restrict	(Optional) Sets the security violation restrict mode. In this mode, a port security violation restricts data and causes the security violation counter to increment.
shutdown	(Optional) Sets the security violation shutdown mode. In this mode, a port security violation causes the interface to immediately become error disabled.

Defaults

The default settings are as follows:

- Port security is disabled.

- When port security is enabled and no keywords are entered, the default maximum number of secure MAC addresses is 1.
- Aging is disabled.
- Aging time is 0 minutes
- All secure addresses on this port age out immediately after they are removed from the secure address list.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(19)EW	Extended to include DHCP snooping security enhancement.
	12.2(18)EW	Add support for sticky interfaces.

Usage Guidelines After you have set the maximum number of secure MAC addresses allowed on a port, you can add secure addresses to the address table by manually configuring them, by allowing the port to dynamically configure them, or by configuring some MAC addresses and allowing the rest to be dynamically configured.

Packets are dropped into hardware when the maximum number of secure MAC addresses are in the address table and a station that does not have a MAC address in the address table attempts to access the interface.

If you enable port security on a voice VLAN port and if there is a PC connected to the IP phone, you set the maximum allowed secure addresses on the port to more than 1.

You cannot configure static secure MAC addresses in the voice VLAN.

A secure port has the following limitations:

- A secure port cannot be a dynamic access port or a trunk port.
- A secure port cannot be a routed port.
- A secure port cannot be a protected port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- A secure port cannot belong to a Fast EtherChannel or Gigabit EtherChannel port group.
- A secure port cannot be an 802.1X port.
- If you try to enable 802.1X on a secure port, an error message appears, and 802.1X is not enabled. If you try to change an 802.1X-enabled port to a secure port, an error message appears, and the security settings are not changed.

When a secure port is in the error-disabled state, you can remove it from this state by entering the **errdisable recovery cause psecure-violation** global configuration command, or you can manually reenble it by entering the **shutdown** and **no shut down** interface configuration commands.

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 becomes 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.

If the sticky command is executed without a MAC address specified, all MAC addresses learned on that port will be made sticky. You can also specify a specific MAC address to be a sticky address by entering the **sticky** keyword next to it.

You can configure the sticky feature even when port security is not enabled on the interface. The feature becomes operational when you enable port security on the interface.

You can use the **no** form of the **sticky** command only if the sticky feature is already enabled on the interface.

Examples

This example shows how to enable port security on Fast Ethernet port 12 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 fastethernet 2/12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)#
```

You can verify the settings for all secure ports or the specified port by using the **show port-security** privileged EXEC command.

This example shows how to make all MAC addresses learned on Fast Ethernet port 12 sticky:

```
Switch(config)# interface fastethernet 2/12
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)
```

This example shows how to make MAC address 1000.2000.3000 sticky on Fast Ethernet port 12:

```
Switch(config)# interface fastethernet 2/12
Switch(config-if)# switchport port-security mac-address sticky 1000.2000.3000
Switch(config-if)
```

This example shows how to disable the sticky feature on Fast Ethernet port 12:

```
Switch(config)# interface fastethernet 2/12
Switch(config-if)# no switchport port-security mac-address sticky
Switch(config-if)
```



Note

This command makes all sticky addresses on this interface normal learned entries. It does not delete the entries from the secure MAC address table.

This example shows how to remove all sticky and static addresses configured on the interface:

```
Switch(config)# interface fastethernet 2/12
Switch(config-if)# no switchport port-security mac-address
Switch(config-if)
```

This example shows how to configure a secure MAC address on Fast Ethernet port 12:

```
Switch(config)# interface fastethernet 0/12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 1000.2000.3000
Switch(config-if)
```

You can verify your settings by using the **show port-security address** privileged EXEC command.

Related Commands

[show interfaces switchport](#)
[show port-security](#)
[switchport block](#)

switchport private-vlan association trunk

To configure the association between a secondary VLANs and a VLAN on a private VLAN trunk port, use the **switchport private-vlan association trunk** command. To remove the private VLAN mapping from the port, use the **no** form of the command.

switchport private-vlan association trunk {*primary-vlan-id*} {*secondary-vlan-id*}

no switchport private-vlan association trunk {*primary-vlan-id*}

Syntax Description

primary-vlan-id Number of the primary VLAN of the PVLAN relationship.

secondary-vlan-id Number of the secondary VLAN of the private VLAN relationship.

Defaults

Private VLAN mapping is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Multiple private VLAN pairs can be specified so that a private VLAN trunk port can carry multiple secondary VLANs. If an association is specified for the existing primary VLAN, the existing association is replaced.

If there is no trunk association, any packets received on secondary VLANs are dropped.

Examples

This example shows how to configure a port with a primary VLAN (VLAN 18) and secondary VLAN (VLAN 20):

```
Switch(config-if)# switchport private-vlan association trunk 18 20
Switch(config-if)#
```

This example shows how to remove the PVLAN association from the port:

```
Switch(config-if)# no switchport private-vlan association trunk 18
Switch(config-if)#
```

Related Commands

[show interfaces switchport](#)
[switchport mode](#)

switchport private-vlan host-association

To define a PVLAN association for an isolated or community port, use the **switchport private-vlan host-association** command. To remove the PVLAN mapping from the port, use the **no** form of the command.

```
switchport private-vlan host-association {primary-vlan-id} {secondary-vlan-id}
```

```
no switchport private-vlan host-association
```

Syntax Description	
<i>primary-vlan-id</i>	Number of the primary VLAN of the PVLAN relationship; valid values are from 1 to 4094.
<i>secondary-vlan-list</i>	Number of the secondary VLAN of the private VLAN relationship; valid values are from 1 to 4094.

Defaults Private VLAN mapping is disabled.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended addressing was added.

Usage Guidelines There is no runtime effect on the port unless it is in PVLAN host mode. If the port is in PVLAN host mode but neither of the VLANs exists, the command is allowed, but the port is made inactive. The secondary VLAN may be an isolated or community VLAN.

Examples This example shows how to configure a port with a primary VLAN (VLAN 18) and secondary VLAN (VLAN 20):

```
Switch(config-if)# switchport private-vlan host-association 18 20
Switch(config-if)#
```

This example shows how to remove the PVLAN association from the port:

```
Switch(config-if)# no switchport private-vlan host-association
Switch(config-if)#
```

Related Commands [show interfaces switchport](#)
[switchport mode](#)

switchport private-vlan mapping

To define private VLAN mapping for a promiscuous port, use the **switchport private-vlan mapping** command. To clear all mapping from the primary VLAN, use the **no** form of this command.

```
switchport private-vlan mapping {primary-vlan-id} {secondary-vlan-list} |
  {add secondary-vlan-list} | {remove secondary-vlan-list}
```

```
no switchport private-vlan mapping
```

Syntax Description

<i>primary-vlan-id</i>	Number of the primary VLAN of the PVLAN relationship; valid values are from 2 to 4094.
<i>secondary-vlan-list</i>	Number of the secondary VLANs to map to the primary VLAN; valid values are from 2 to 4094.
add	Maps the secondary VLANs to the primary VLAN.
remove	Clears mapping between secondary VLANs and the primary VLAN.

Defaults

Private VLAN mapping is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Support for extended addressing was added.

Usage Guidelines

There is no runtime effect on the port unless it is in PVLAN promiscuous mode. If the port is in PVLAN promiscuous mode but the VLANs do not exist, the command is allowed, but the port is made inactive. The secondary VLAN may be an isolated or community VLAN.

Examples

This example shows how to configure the mapping of primary VLAN 18 to secondary isolated VLAN20 on a port:

```
Switch(config-if)# switchport private-vlan mapping 18 20
Switch(config-if)#
```

This example shows how to add a VLAN to the mapping:

```
Switch(config-if)# switchport private-vlan mapping 18 add 21
Switch(config-if)#
```

Related Commands

[show interfaces private-vlan mapping](#)

switchport private-vlan trunk allowed vlan

To configure a list of allowed normal VLANs on a private VLAN trunk port, use the **switchport private-vlan trunk allowed vlan** command. To remove all allowed normal VLANs from a private VLAN trunk port, use the **no** form of the command.

```
switchport private-vlan trunk allowed vlan {vlan-list} all | none | [add | remove | except]
vlan_atom [,vlan_atom...]
```

```
no switchport private-vlan trunk allowed vlan
```

Syntax Description		
	<i>vlan_list</i>	Sets the list of allowed VLANs. See “Usage Guidelines” for formatting guidelines for <i>vlan_list</i> .
	all	Specifies all VLANs from 1 to 4094. This keyword is not supported on commands that do not permit all VLANs in the list to be set at the same time.
	none	Indicates an empty list. This keyword is not supported on commands that require certain VLANs to be set or at least one VLAN to be set.
	add	(Optional) Adds the defined list of VLANs to those currently set instead of replacing the list.
	remove	(Optional) Removes the defined list of VLANs from those currently set instead of replacing the list.
	except	(Optional) Lists the VLANs that should be calculated by inverting the defined list of VLANs.
	<i>vlan_atom</i>	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 All allowed normal VLANs are removed from a private VLAN trunk port.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines By default, no normal VLANs are allowed unless explicitly configured to be allowed.

Only use this command for normal VLANs on a private VLAN trunk port.

Use the **switchport private-vlan association trunk** command to configure a port that can carry private VLANs on a private VLAN trunk port.

Examples

This example shows how to configure private VLAN trunk port that carries normal VLANs 1 to10:

```
Switch(config-if)# switchport private-vlan trunk allowed vlan 1-10  
Switch(config-if)#
```

This example shows how to remove all allowed normal VLANs from a private VLAN trunk port:

```
Switch(config-if)# no switchport private-vlan trunk allowed vlan  
Switch(config-if)#
```

Related Commands

[show interfaces switchport](#)
[switchport mode](#)

switchport private-vlan trunk native vlan

To control the tagging of native VLAN traffic on 802.1Q private VLAN trunks, use the **switchport private-vlan trunk native vlan tag** command. To remove the control of tagging (and default to the global setting), use the **no** form of the command.

switchport private-vlan trunk native vlan tag

no switchport private-vlan trunk native vlan tag

Syntax Description This command has no arguments or keywords.

Defaults The default setting is global; the settings on the port are determined by the global setting.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(18)EW	Removed vlan-id keyword.

Usage Guidelines The configuration created with this command only applies to ports that are configured as private VLAN trunks.

Examples This example shows how to enable 802.1Q native VLAN tagging on a PVLAN trunk:

```
Switch(config-if)# switchport private-vlan trunk native vlan tag
Switch(config-if)#
```

Related Commands [show interfaces switchport](#)
[switchport mode](#)

switchport trunk

To set trunk characteristics when an interface is in trunking mode, use the **switchport trunk** command. To reset all of the trunking characteristics back to the original defaults, use the **no** form of this command.

switchport trunk encapsulation {isl | dot1q | negotiate}

no switchport trunk encapsulation

switchport trunk native vlan {tag | vlan_id}

no switchport trunk native vlan {tag | vlan_id}

switchport trunk allowed vlan vlan_list

no switchport trunk allowed vlan vlan_list

switchport trunk pruning vlan vlan_list

no switchport trunk pruning vlan vlan_list

Syntax Description

encapsulation isl	Sets the trunk encapsulation format to ISL.
encapsulation dot1q	Sets the trunk encapsulation format to 802.1Q.
encapsulation negotiate	Specifies that if DISL and DTP negotiation do not resolve the encapsulation format, ISL will be the selected format.
native vlan tag	Specifies the tagging of native VLAN traffic on 802.1Q trunks.
native vlan vlan_id	Sets the native VLAN for the trunk in 802.1Q trunking mode.
allowed vlan vlan_list	Sets the list of allowed VLANs that transmit this interface in tagged format when in trunking mode. See “Usage Guidelines” for formatting guidelines for <i>vlan_list</i> .
pruning vlan vlan_list	Sets the list of VLANs that are enabled for VTP pruning when the switch is in trunking mode. See “Usage Guidelines” for formatting guidelines for <i>vlan_list</i> .

Defaults

The default settings are as follows:

- Encapsulation type is dependent on the platform or interface hardware.
- Access VLANs and trunk interface native VLANs are a default VLAN corresponding to the platform or interface hardware.
- All VLAN lists include all VLANs.
- Native VLAN tagging is enabled on the port if enabled globally.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Support for extended addressing was added.
12.2(18)EW	Support for native VLAN tagging was added.

Usage Guidelines

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 supported on commands that do not permit all VLANs in the list to be set at the same time.
- **none** indicates an empty list. This keyword is not supported 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.
- **remove** removes the defined list of VLANs from those currently set, instead of replacing the list.
- **except** lists the VLANs that should be calculated by inverting the defined list of VLANs.
- *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.

The **switchport trunk encapsulation** command is supported only for platforms and interface hardware that can support both ISL and 802.1Q formats.

If you enter the **negotiate** keywords, and DISL and DTP negotiation do not resolve the encapsulation format, ISL is the selected format. The **no** form of the command resets the trunk encapsulation format back to the default.

The **no** form of the **native vlan** command resets the native mode VLAN to the appropriate default VLAN for the device.

The **no** form of the **allowed vlan** command resets the list to the default list, which allows all VLANs.

The **no** form of the **pruning vlan** command resets the list to the default list, which enables all VLANs for VTP pruning.

The following configuration guidelines and restrictions apply when using 802.1Q trunks and impose some limitations on the trunking strategy for a network. Keep these restrictions and suggestions in mind when using 802.1Q trunks:

- When connecting Cisco switches through an 802.1Q trunk, make sure the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning tree loops might result.
- Disabling spanning tree on the native VLAN of an 802.1Q trunk without disabling spanning tree on every VLAN in the network can cause spanning tree loops. We recommend that you leave spanning tree enabled on the native VLAN of an 802.1Q trunk. If this is not possible, disable spanning tree on every VLAN in the network. Make sure your network is free of physical loops before disabling spanning tree.
- When you connect two Cisco switches through 802.1Q trunks, the switches exchange spanning tree BPDUs on each VLAN allowed on the trunks. The BPDUs on the native VLAN of the trunk are sent untagged to the reserved IEEE 802.1d spanning tree multicast MAC address (01-80-C2-00-00-00). The BPDUs on all other VLANs on the trunk are sent tagged to the reserved SSTP multicast MAC address (01-00-0c-cc-cc-cd).

- Non-Cisco 802.1Q switches maintain only a single instance of spanning tree (MST) that defines the spanning tree topology for all VLANs. When you connect a Cisco switch to a non-Cisco switch through an 802.1Q trunk, the MST of the non-Cisco switch and the native VLAN spanning tree of the Cisco switch combine to form a single spanning tree topology known as the CST.
- Because Cisco switches transmit BPDUs to the SSTP multicast MAC address on VLANs other than the native VLAN of the trunk, non-Cisco switches do not recognize these frames as BPDUs and flood them on all ports in the corresponding VLAN. Cisco switches connected to the non-Cisco 802.1Q network receive these flooded BPDUs. Because Cisco switches receive the flooded BPDUs the switches can maintain a per-VLAN spanning tree topology across a network of non-Cisco 802.1Q switches. The non-Cisco 802.1Q network separating the Cisco switches is treated as a single broadcast segment between all switches connected to the non-Cisco 802.1Q network through 802.1Q trunks.
- Ensure that the native VLAN is the same on *all* of the 802.1Q trunks connecting the Cisco switches to the non-Cisco 802.1Q network.
- If you are connecting multiple Cisco switches to a non-Cisco 802.1Q network, all of the connections must be through 802.1Q trunks. You cannot connect Cisco switches to a non-Cisco 802.1Q network through ISL trunks or through access ports. This action causes the switch to place the ISL trunk port or access port into the spanning tree “port inconsistent” state and no traffic will pass through the port.

For native VLAN tagging, the following guidelines apply:

- The **no switchport trunk native vlan tag** command disables the native VLAN tagging operation on a port. This overrides the global tagging configuration.
- The **switchport trunk native vlan tag** command can be used to reenables tagging on a disabled port.
- The **no** option is saved to NVRAM so that the user does not have to manually select the ports to disable the tagging operation each time the switch reboots.
- When the **switchport trunk native vlan tag** command is enabled and active, all packets on the native VLAN are tagged, and incoming untagged data packets are dropped. Untagged control packets are accepted.

Examples

This example shows how to cause a port interface 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
Switch(config-if)#
```

This example shows how to enable 802.1Q tagging on a port:

```
Switch(config-if)# switchport trunk native vlan tag
Switch(config-if)#
```

Related Commands

[show interfaces switchport](#)

system mtu

To set the maximum Layer 2 or Layer 3 payload size, use the **system mtu** command. To revert to the default MTU setting, use the **no** form of this command.

system mtu *datagram-size*

no system mtu

Syntax Description	<i>datagram-size</i> Specifies the Layer 2 payload size; valid values from 1500 to 1552 bytes.
---------------------------	--

Defaults	The default MTU setting is 1500 bytes.
-----------------	--

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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	<p>The <i>datagram-size</i> parameter specifies the Ethernet payload size, not the total Ethernet frame size, and the Layer 3 MTU is changed as a result of changing the system mtu command.</p> <p>For ports from 3 to 18 on linecard model WS-X4418-GB and ports from 1 to 12 on model WS-X4412-2GB-TX, only the standard IEEE Ethernet payload size of 1500 bytes is supported.</p> <p>For other modules, an Ethernet payload size of up to 1552 bytes is supported, with a total Ethernet frame size of up to 1600 bytes.</p>
-------------------------	--

Examples	<p>This example shows how to set the MTU size to 1550 bytes:</p> <pre>Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# system mtu 1550 Switch(config)# end Switch#</pre>
-----------------	---

	<p>This example shows how to revert to the default MTU setting:</p> <pre>Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# no system mtu Switch(config)# end Switch#</pre>
--	--

Related Commands	<p>show interfaces</p> <p>show system mtu</p>
-------------------------	---

tracert mac

To display the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address, use the **tracert mac** command.

```
tracert 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) Source or destination switch interface.
<i>source-mac-address</i>	MAC address of the source switch in hexadecimal format.
<i>destination-mac-address</i>	MAC address of the destination switch in hexadecimal format.
vlan <i>vlan-id</i>	(Optional) 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. Do not enter leading zeros.
detail	(Optional) Displays detail information.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(15)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Do not use leading zeros when entering a VLAN ID.

The Layer 2 tracert feature is available on these switches:

- Catalyst 2950 switches running Release 12.1(12c)EA1 or later
- Catalyst 3550 switches running Release 12.1(12c)EA1 or later
- Catalyst4500 series switches running Catalyst operating system Release 6.2 or later for the supervisor engine
- Catalyst4500 series switches running Release 12.1(15)EW or later
- Catalyst 5000 family switches running Catalyst operating system Release 6.1 or later for the supervisor engine
- Catalyst 6500 series switches running Catalyst operating system Release 6.1 or later for the supervisor engine

For Layer 2 tracert to functional properly, Cisco Discovery Protocol (CDP) must be enabled on all of 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 tracert, the switch continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

Layer 2 traceroute supports only unicast traffic. If you specify a multicast source or destination MAC address, the physical path is not identified, and an error message appears.

The **traceroute mac** command output shows the Layer 2 path when the specified source and destination addresses belong to the same VLAN. If you specify source and destination addresses that belong to different VLANs, the Layer 2 path is not identified, and an error message appears.

If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong. If the VLAN is not specified, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port). When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display the Layer 2 path by specifying the source and destination MAC addresses:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 (2.2.6.6) :Fa0/1 =>Fa0/3
con5          (2.2.5.5       ) : Fa0/3 =>Gi0/1
con1          (2.2.1.1       ) : Gi0/1 =>Gi0/2
con2          (2.2.2.2       ) : Gi0/2 =>Fa0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
Switch#
```

This example shows how to display the detailed Layer 2 path:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201 detail
Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / WS-C2950G-24-EI / 2.2.6.6 :
      Fa0/1 [auto, auto] =>Fa0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
      Fa0/3 [auto, auto] =>Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
      Gi0/1 [auto, auto] =>Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
      Gi0/2 [auto, auto] =>Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
Switch#
```

This example shows the Layer 2 path when the switch is not connected to the source switch:

```
Switch# traceroute mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source ....
Source 0000.0201.0501 found on con5[WS-C2950G-24-EI] (2.2.5.5)
con5 / WS-C2950G-24-EI / 2.2.5.5 :
      Fa0/1 [auto, auto] =>Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
      Gi0/1 [auto, auto] =>Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
      Gi0/2 [auto, auto] =>Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
Switch#
```

This example shows the Layer 2 path when the switch cannot find the destination port for the source MAC address:

```
Switch# tracroute mac 0000.0011.1111 0000.0201.0201
Error:Source Mac address not found.
Layer2 trace aborted.
Switch#
```

This example shows the Layer 2 path when the source and destination devices are in different VLANs:

```
Switch# tracroute mac 0000.0201.0601 0000.0301.0201
Error:Source and destination macs are on different vlans.
Layer2 trace aborted.
Switch#
```

This example shows the Layer 2 path when the destination MAC address is a multicast address:

```
Switch# tracroute mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
Switch#
```

This example shows the Layer 2 path when source and destination switches belong to multiple VLANs:

```
Switch# tracroute mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace aborted.
Switch#
```

This example shows how to display the Layer 2 path by specifying the interfaces on the source and destination switches:

```
Switch# tracroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3 0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 (2.2.6.6) :Fa0/1 =>Fa0/3
con5          (2.2.5.5      ) : Fa0/3 =>Gi0/1
con1          (2.2.1.1      ) : Gi0/1 =>Gi0/2
con2          (2.2.2.2      ) : Gi0/2 =>Fa0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
Switch#
```

Related Commands [tracroute mac ip](#)

traceroute mac ip

To display the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname, use the **traceroute mac** command.

```
traceroute mac ip {source-ip-address | source-hostname} {destination-ip-address | destination-hostname} [detail]
```

Syntax Description		
<i>source-ip-address</i>		IP address of the source switch as a 32-bit quantity in dotted-decimal format.
<i>destination-ip-address</i>		IP address of the destination switch as a 32-bit quantity in dotted-decimal format.
<i>source-hostname</i>		IP hostname of the source switch.
<i>destination-hostname</i>		IP hostname of the destination switch.
detail		(Optional) Displays detailed traceroute MAC IP information.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines The Layer 2 traceroute feature is available on these switches:

- Catalyst 2950 switches running Release 12.1(12c)EA1 or later
- Catalyst 3550 switches running Release 12.1(12c)EA1 or later
- Catalyst4500 series switches running Catalyst operating system Release 6.2 or later for the supervisor engine
- Catalyst4500 series switches running Release 12.1(15)EW or later
- Catalyst 5000 family switches running Catalyst operating system Release 6.1 or later for the supervisor engine
- Catalyst 6500 series switches running Catalyst operating system Release 6.1 or later for the supervisor engine

For Layer 2 traceroute to functional 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 **tracert mac ip** command output shows the Layer 2 path when the specified source and destination IP addresses are in the same subnet. When you specify the IP addresses, the switch uses Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.

- If an ARP entry exists for the specified IP address, the switch uses the associated MAC address and identifies the physical path.
- If an ARP entry does not exist, the switch sends an ARP query and tries to resolve the IP address. The IP addresses must be in the same subnet. If the IP address is not resolved, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port). When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display the Layer 2 path by specifying the source and destination IP addresses and by using the **detail** keyword:

```
Switch# tracert mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac....
2.2.66.66 =>0000.0201.0601
2.2.22.22 =>0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / WS-C2950G-24-EI / 2.2.6.6 :
    Fa0/1 [auto, auto] =>Fa0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
    Fa0/3 [auto, auto] =>Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
    Gi0/1 [auto, auto] =>Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
    Gi0/2 [auto, auto] =>Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
Switch#
```

This example shows how to display the Layer 2 path by specifying the source and destination hostnames:

```
Switch# tracert 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) :Fa0/1 =>Fa0/3
con5          (2.2.5.5      ) :   Fa0/3 =>Gi0/1
con1          (2.2.1.1      ) :   Gi0/1 =>Gi0/2
con2          (2.2.2.2      ) :   Gi0/2 =>Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
Switch#
```

This example shows the Layer 2 path when Address Resolution Protocol (ARP) cannot associate the source IP address with the corresponding MAC address:

```
Switch# tracert mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
Switch#
```

Related Commands [traceroute mac](#)

tx-queue

To configure the transmit queue parameters for an interface, use the **tx-queue** command. To return to the default value, use the **no** form of this command.

```
tx-queue [queue-id] {bandwidth bandwidth-rate | priority high | shape shape-rate}
```

```
no tx-queue
```

Syntax Description	
<i>queue-id</i>	(Optional) Number of the queue; valid values are from 1 to 4.
bandwidth <i>bandwidth-rate</i>	Specifies traffic bandwidth; valid values are from 16000 to 1000000000 bits per second.
priority high	Specifies high priority.
shape <i>shape-rate</i>	Specifies the maximum rate that packets are passed through a transmit queue; valid values are from 16000 to 1000000000 bits per second.

Defaults

The default settings are as follows:

- Encapsulation type is dependent on the platform or interface hardware.
- QoS enabled bandwidth rate is 4:255.
- QoS disabled bandwidth rate is 255:1.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The bandwidth and shape rates cannot exceed the maximum speed of the interface.

Bandwidth can be configured only on the following:

- Uplink ports on Supervisor Engine III (WS-X4014)
- Ports on the WS-X4306-GB module
- The two 1000BASE-X ports on the WS-X4232-GB-RJ module
- The first two ports on the WS-X4418-GB module
- The two 1000BASE-X ports on the WS-X4412-2GB-TX module

Only transmit queue 3 can be configured to be a high-priority transmit queue.

Examples

This example shows how to allocate bandwidth on queue 1 to 100 MBPS:

```
Switch(config-if)# tx-queue 1
```

```
Switch(config-if-tx-queue)# bandwidth 1000000000  
Switch(config-if-tx-queue)#
```

This example shows how to configure transmit queue 3 to the high priority:

```
Switch(config-if)# tx-queue 3  
Switch(config-if-tx-queue)# priority high  
Switch(config-if-tx-queue)#
```

This example shows how to configure the traffic shaping rate of 64 kbps to transmit queue 1:

```
Switch(config-if)# tx-queue 1  
Switch(config-if-tx-queue)# shape 64000  
Switch(config-if-tx-queue)#
```

Related Commands [show qos interface](#)

udld (global configuration mode)

To enable aggressive or normal mode in the UDLD protocol and to set the configurable message timer time, use the **udld** command. Use the **no** form of the command to do the following:

- Disable normal mode UDLD on all fiber ports by default
- Disable aggressive mode UDLD on all fiber ports by default
- Disable the message timer

udld enable | aggressive

no udld enable | aggressive

udld message time *message-timer-time*

no udld message time

Syntax Description	enable	Enables UDLD in normal mode by default on all fiber interfaces.
	aggressive	Enables UDLD in aggressive mode by default on all fiber interfaces.
	message time <i>message-timer-time</i>	Sets the period of time between the UDLD probe messages on ports that are in advertisement mode and are currently determined to be bidirectional; valid values are from 7 to 90 seconds.

Defaults All fiber interfaces are disabled and the message timer time equals 15 seconds.

Command Modes Global configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines If you enable aggressive mode, once all the neighbors of a port have aged out either in the advertisement or in the detection phase, UDLD restarts the linkup sequence to try to resynchronize with any potentially out-of-sync neighbor and shuts down the port if the message train from the link is still undetermined.

This command affects fiber interfaces only. Use the **udld (interface configuration mode)** command to enable UDLD on other interface types.

Examples This example shows how to enable UDLD on all fiber interfaces:

```
Switch (config)# udld enable
Switch (config)#
```

Related Commands[show udld](#)[udld \(interface configuration mode\)](#)

udd (interface configuration mode)

To enable UDLD on an individual interface or to prevent a fiber interface from being enabled by the **udd (global configuration mode)** command, use the **udd** command. To return to the **udd (global configuration mode)** command setting, or if the port is a nonfiber port to disable UDLD, use the **no** form of this command.

udd { enable | aggressive | disable }

no udd { enable | aggressive | disable }

Syntax Description

enable	Enables UDLD on this interface.
aggressive	Enables UDLD in aggressive mode on this interface.
disable	Disables UDLD on this interface.

Defaults

The fiber interfaces are enabled per the state of the global **udd (enable or aggressive)** command, and the nonfiber interfaces are enabled with UDLD disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

If you enable aggressive mode, once all the neighbors of a port have aged out either in the advertisement or in the detection phase, UDLD restarts the linkup sequence to try to resynchronize with any potentially out-of-sync neighbor and shuts down the port if the message train from the link is still undetermined.

Use the **no udd enable** command on fiber ports to return control of UDLD to the global **udd enable** command or to disable UDLD on nonfiber ports.

Use the **udd aggressive** command on fiber ports to override the setting of the global **udd (enable or aggressive)** command. Use the **no** form on fiber ports to remove this setting, return control of UDLD enabling back to the global **udd** command or to disable UDLD on nonfiber ports.

The **disable** keyword is supported on fiber ports only. Use the **no** form of this command to remove this setting and return control of UDLD to the **udd (global configuration mode)** command.

If the port changes from fiber to nonfiber or vice versa, all configurations will be maintained because of a change of module or a GBIC change detected by the platform software.

Examples

This example shows how to cause any port interface to enable UDLD, despite the current global **udd (global configuration mode)** setting:

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


This example shows how to cause any port interface to enable UDLD in aggressive mode, despite the current global **udld (enable or aggressive)** setting:

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

This example shows how to cause a fiber port interface to disable UDLD, despite the current global **udld (global configuration mode)** setting:

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

Related Commands

show udld
udld (global configuration mode)

udld reset

To reset all UDLD ports in the shutdown state, use the **udld reset** command.

udld reset

Syntax Description This command has no keywords or variables.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines If the interface configuration is still enabled for UDLD, these ports will begin to run UDLD again and may shut down if the reason for the shutdown has not been corrected.

The **udld reset** command permits traffic to flow on the ports again; other features, such as spanning tree, PAGP, and DTP, operate normally if enabled.

Examples This example shows how to reset all ports shut down by UDLD:

```
Switch# udld reset
Switch#
```

Related Commands [show udld](#)

unidirectional

To configure nonblocking Gigabit Ethernet ports to unidirectionally send or receive traffic on an interface, use the **unidirectional** command. To disable unidirectional communication, use the **no** form of this command.

unidirectional {**receive-only** | **send-only**}

no unidirectional {**receive-only** | **send-only**}

Syntax Description	receive-only	Specifies unidirectional reception.
	send-only	Specifies unidirectional transmission.

Defaults Disabled

Command Modes Interface configuration

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Enabling port unidirectional mode automatically disables port UDLD. You must manually ensure that the unidirectional link does not create a spanning tree loop in the network.

Examples This example shows how to set Gigabit Ethernet interface 1/1 to receive traffic unidirectionally:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# unidirectional receive-only
Switch(config-if)# end
Switch#
```

Related Commands [show interfaces switchport](#)

username

To establish a username-based authentication system, use the **username** command.

username *name* **secret** { **0** | **5** } *password*

Syntax Description	
<i>name</i>	User ID of the user.
secret 0 5	Specifies the authentication system for the user; valid values are 0 (text immediately following is not encrypted) and 5 (text immediately following is encrypted using an MD5-type encryption method).
<i>password</i>	Password of the user.

Defaults No username-based authentication system is established.

Command Modes Global configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Use this command to enable enhanced password security for the specified username. This command enables MD5 encryption on the password. MD5 encryption is a strong encryption method that is not retrievable. You cannot use MD5 encryption with protocols that require clear-text passwords, such as CHAP.

You can use this command for defining usernames that get special treatment. For example, you can define an “info” username that does not require a password but that connects the user to a general-purpose information service.

The **username** command provides both username and **secret** authentication for login purposes only.

The *name* argument can be only one word. White spaces and quotation marks are not allowed.

You can use multiple **username** commands to specify options for a single user.

For information about additional **username** commands, refer to the *Cisco IOS Command Reference*.

Examples This example shows how to specify an MD5 encryption on a password (warrior) for a username (xena):

```
Switch(config)# username xena secret 5 warrior
Switch(config)#
```

Related Commands

- enable password** (refer to Cisco IOS documentation)
- enable secret** (refer to Cisco IOS documentation)
- username** (refer to Cisco IOS documentation)

verify

To verify the checksum of a file on a Flash memory file system, use the **verify** command.

```
verify [/md5] [flash-filesystem:] [filename] [expected-md5-signature]
```

Syntax Description		
	/md5	(Optional) Verifies MD5 signatures.
	<i>flash-filesystem:</i>	(Optional) Device where the Flash resides; valid values are bootflash: , slot0: , flash: , or sup-bootflash: .
	<i>filename</i>	(Optional) Name of the Cisco IOS image.
	<i>expected-md5-signature</i>	(Optional) MD5 signature.

Defaults The current working device is specified.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Each software image that is distributed on disk uses a single checksum for the entire image. This checksum is displayed only when the image is copied into Flash memory.

The Readme file, which is included with the image on the disk, lists the name, file size, and checksum of the image. Review the contents of the Readme file before loading or duplicating the new image so that you can verify the checksum when you copy it into Flash memory or on to a server.

Use the **verify /md5** command to verify the MD5 signature of a file before using it. This command validates the integrity of a copied file by comparing a precomputed MD5 signature with the signature computed by this command. If the two MD5 signatures match, the copied file is identical to the original file.

You can find the MD5 signature posted on the Cisco.com page with the image.

You can use the **verify /md5** command in one of the following ways:

- Verify the MD5 signatures manually by entering the **verify /md5 filename** command.

Check the displayed signature against the MD5 signature posted on the Cisco.com page.

- Allow the system to compare the MD5 signatures by entering the **verify /md5 {flash-filesystem:filename} {expected-md5-signature}** command.

After completing the comparison, the system returns with a verified message. If an error is detected, the output is similar to the following:

```
Switch# verify /md5 slot0:c4-jsv-mz 0f
.....
.....
.....
.....
```

```

.....
.....Done!
%Error verifying slot0:c4-jsv-mz
Computed signature   = 0f369ed9e98756f179d4f29d6e7755d3
Submitted signature = 0f

```

To display the contents of Flash memory, enter the **show flash** command. The Flash contents listing does not include the checksum of individual files. To recompute and verify the image checksum after the image has been copied into Flash memory, enter the **verify** command.

A colon (:) is required after the specified device.

Examples

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

```

Switch# verify cat6k_r47_1.cbi
.....
File cat6k_r47_1.cbi verified OK.
Switch#

```

This example shows how to manually check the MD5 signature:

```

Switch# verify /md5 c4-jsv-mz
.....
.....
.....Done!
verify /md5 (slot0:c4-jsv-mz) = 0f369ed9e98756f179d4f29d6e7755d3
Switch#

```

This example shows how to allow the system to compare the MD5 signatures:

```

Switch# verify /md5 slot0:c4-jsv-mz 0f369ed9e98756f179d4f29d6e7755d3
.....
.....
.....Done!
verified /md5 (slot0:c6sup12-jsv-mz) = 0f369ed9e98756f179d4f29d6e7755d3
Switch#

```

Related Commands

show file system (Flash file system) (refer to Cisco IOS documentation)
show flash (refer to Cisco IOS documentation)

vlan (VLAN Database mode)

To configure a specific VLAN, use the **vlan** command. To delete a VLAN, use the **no** form of this command.

```
vlan vlan_id [are hops] [backupcrfmode] [bridge type / bridge-num] [media type] [mtu mtu-size]
[name vlan-name] [parent parent-vlan-id] [ring ring-number] [said said-value] [state
{suspend | active}] [stp type type] [tb-vlan1 tb-vlan1-id] [tb-vlan2 tb-vlan2-id]
```

```
no vlan vlan
```

Syntax	Description
<i>vlan_id</i>	Number of the VLAN; valid values are from 1 to 4094.
are <i>hops</i>	(Optional) Specifies the maximum number of All Route Explorer hops for this VLAN; valid values are from 0 to 13. Zero is assumed if no value is specified.
backupcrfmode	(Optional) Enables or disables the backup CRF mode of the VLAN; valid values are enable and disable .
bridge <i>type</i>	(Optional) Specifies the bridging characteristics of the VLAN or identification number of the bridge; valid <i>type</i> values are srb and srt .
<i>bridge_num</i>	(Optional) Valid <i>bridge_num</i> values are from 0 to 15.
media <i>type</i>	(Optional) Specifies the media type of the VLAN; valid values are fast ethernet , fd-net , fddi , trcrf , and trbrf .
mtu <i>mtu-size</i>	(Optional) Specifies the maximum transmission unit (packet size, in bytes) that the VLAN can use; valid values are from 576 to 18190.
name <i>vlan-name</i>	(Optional) Defines a text string used as the name of the VLAN (1to32characters).
parent <i>parent-vlan-id</i>	(Optional) Specifies the ID number of the parent VLAN of FDDI or Token Ring-type VLANs; valid values are from 2 to 1001.
ring <i>ring-number</i>	(Optional) Specifies the ring number of FDDI or Token Ring-type VLANs; valid values are from 2 to 1001.
said <i>said-value</i>	(Optional) Specifies the security association identifier; valid values are from 1 to 4294967294.
state	(Optional) Specifies the state of the VLAN.
suspend	Specifies that the state of the VLAN is suspended. VLANs in the suspended state do not pass packets.
active	Specifies that the state of the VLAN is active.
stp type <i>type</i>	(Optional) Specifies the STP type; valid values are ieee , ibm , and auto .
tb-vlan1 <i>tb-vlan1-id</i>	(Optional) Specifies the ID number of the first translational VLAN for this VLAN; valid values are from 2 to 1001. Zero is assumed if no value is specified.
tb-vlan2 <i>tb-vlan2-id</i>	(Optional) Specifies the ID number of the second translational VLAN for this VLAN; valid values are from 2 to 1001. Zero is assumed if no value is specified.

Defaults

The defaults are as follows:

- The *vlan-name* is “VLANxxxx” where “xxxx” represents four numeric digits (including leading zeroes) equal to the VLAN ID number.
- The *media* type is Fast Ethernet.
- The state is active.
- The *said-value* is 100,000 plus the VLAN ID number.
- The *mtu-size* default is dependent upon the VLAN type:
 - *fddi*—1500
 - *trcrf*—1500 if V2 is not enabled; 4472 if it is enabled
 - *fd-net*—1500
 - *trbrf*—1500 if V2 is not enabled; 4472 if it is enabled
- No ring number is specified.
- No bridge number is specified.
- No parent VLAN is specified.
- No STP type is specified.
- No translational bridge VLAN is specified.

Command Modes

VLAN configuration

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

VLAN 1 parameters are factory configured and cannot be changed.

When you define *vlan-name*, the name must be unique within the administrative domain.

The SAID is documented in 802.10. When the **no** form is used, the VLANs SAID is returned to the default.

When you define the *said-value*, the name must be unique within the administrative domain.

The **bridge** *bridge-number* argument is used only for Token Ring-net and FDDI-net VLANs and is ignored in other types of VLANs. When the **no** form is used, the VLANs source-route bridging number returns to the default.

The parent VLAN resets to the default if the parent VLAN is deleted or the **media** keyword changes the VLAN type or the VLAN type of the parent VLAN.

The *tb-vlan1* and *tb-vlan2* are used to configure translational bridge VLANs of a specified type of VLAN and are not allowed in other types of VLANs. Translational bridge VLANs must be a different VLAN type than the affected VLAN; if two VLANs are specified, the two must be different VLAN types.

A translational bridge VLAN will reset to the default if the translational bridge VLAN is deleted or the **media** keyword changes the VLAN type or the VLAN type of the corresponding translational bridge VLAN.

Examples

This example shows how to add a new VLAN with all default parameters to the new VLAN database:

```
Switch(vlan)# vlan 2
```

**Note**

If the VLAN already exists, no action occurs.

This example shows how to cause the device to add a new VLAN, specify the media type and parent VLAN ID number 3, and set all other parameters to the defaults:

```
Switch(vlan)# vlan 2 media fastethernet parent 3
VLAN 2 modified:
  Media type FASTETHERNET
  Parent VLAN 3
```

This example shows how to delete VLAN 2:

```
Switch(vlan)# no vlan 2
Switch(vlan)#
```

This example shows how to return the MTU to the default for its type and the translational bridging VLANs to the default:

```
Switch(vlan)# no vlan 2 mtu tb-vlan1 tb-vlan2
Switch(vlan)#
```

Related Commands

[show vlan](#)

vlan access-map

To enter the VLAN access-map command mode to create a VLAN access map, use the **vlan access-map** command. To remove a mapping sequence or the entire map, use the **no** form of this command.

vlan access-map *name* [*seq#*]

no vlan access-map *name* [*seq#*]

Syntax Description

<i>name</i>	VLAN access-map tag.
<i>seq#</i>	(Optional) Map sequence number; valid values are from 0 to 65535.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

If you enter the sequence number of an existing map sequence, you enter VLAN access-map mode. If you do not specify a sequence number, a number is automatically assigned. You can enter one match clause and one action clause per map sequence. If you enter the **no vlan access-map name [seq#]** command without entering a sequence number, the whole map is removed. Once you enter VLAN access-map mode, the following commands are available:

- **action**—Sets the action to be taken (forward or drop).
- **default**—Returns a command to its default settings.
- **end**—Exits from configuration mode.
- **exit**—Exits from VLAN access-map configuration mode.
- **match**—Sets the values to match (IP address or MAC address).
- **no**—Negates a command or reset its defaults.

Examples

This example shows how to enter the VLAN access-map mode:

```
Switch(config)# vlan access-map cisco
Switch(config-access-map)#
```

Related Commands

[match](#)
[show vlan access-map](#)

vlan database

To enter VLAN configuration mode, use the **vlan database** command.

vlan database

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines From VLAN configuration mode, you can access the VLAN database editing buffer manipulation commands, including:

- **abort**—Exits mode without applying the changes.
- **apply**—Applies current changes and bumps the revision number.
- **exit**—Applies changes, bumps the revision number, and exits VLAN configuration mode.
- **no**—Negates a command or sets its defaults; valid values are **vlan** and **vtp**.
- **reset**—Abandons current changes and rereads the current database.
- **show**—Displays the database information.
- **vlan**—Accesses subcommands to add, delete, or modify values that are associated with a single VLAN. For information about the **vlan** subcommands, see the [vlan \(VLAN Database mode\)](#) command.
- **vtp**—Accesses subcommands to perform VTP administrative functions. For information about the **vtp** subcommands, see the [vtp client](#) command.

Examples This example shows how to enter VLAN configuration mode:

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

This example shows how to exit VLAN configuration mode without applying changes after you are in VLAN configuration mode:

```
Switch(vlan)# abort
Aborting...
Switch#
```

This example shows how to delete a VLAN after you are in VLAN configuration mode:

```
Switch(vlan)# no vlan 100
Deleting VLAN 100...
Switch(vlan)#
```

This example shows how to turn off pruning after you are in VLAN configuration mode:

```
Switch(vlan)# no vtp pruning
Pruning switched OFF
Switch(vlan)#
```

Related Commands [show vlan](#)

vlan dot1q tag native

To enable tagging of native VLAN frames on all 802.1Q trunk ports, use the **vlan dot1q tag native** command. Use the **no** form of this command to disable tagging of native VLAN frames.

vlan dot1q tag native

no vlan dot1q tag native

Syntax Description This command has no arguments or keywords.

Defaults The 802.1Q native VLAN tagging is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.2(18)EW	This command was first introduced on the Catalyst 4500 series switch.

Usage Guidelines When enabled, native VLAN packets exiting all 802.1Q trunk ports are tagged unless the port is explicitly configured to disable native VLAN tagging.

When disabled, native VLAN packets exiting all 802.1Q trunk ports are not tagged.

You can use this command with the 802.1Q tunneling feature. This feature operates on an edge switch of a service-provider network and expands VLAN space by using a VLAN-in-VLAN hierarchy and by tagging the tagged packets. You must use 802.1Q trunk ports for sending out packets to the service-provider network. However, packets going through the core of the service-provider network might also be carried on 802.1Q trunks. If the native VLANs of an 802.1Q trunk match the native VLAN of a tunneling port on the same switch, traffic on the native VLAN is not tagged on the sending trunk port. This command ensures that native VLAN packets on all 802.1Q trunk ports are tagged.

Examples This example shows how to enable 802.1Q tagging on native VLAN frames and verify the configuration:

```
Switch# config terminal
Switch (config)# vlan dot1q tag native
Switch (config)# end
Switch# show vlan dot1q tag native
dot1q native vlan tagging is enabled
```

Related Commands [switchport private-vlan trunk native vlan](#)
[switchport trunk](#)

vlan filter

To apply a VLAN access map, use the **vlan filter** command. To clear the VLAN access maps from VLANs or interfaces, use the **no** form of this command.

```
vlan filter map-name {vlan-list vlan-list}
```

```
no vlan filter map-name {vlan-list [vlan-list]}
```

Syntax Description	<i>map-name</i>	VLAN access-map tag.
	vlan-list <i>vlan-list</i>	VLAN list; see “Usage Guidelines” for valid values.

Defaults This command has no default settings.

Command Modes Global configuration

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines When configuring an action clause in a VLAN access map, note the following:

- You can apply the VLAN access map to one or more VLANs.
- The *vlan-list* parameter can be a single VLAN ID, a list of VLAN IDs, or VLAN ID ranges (*vlan-id-vlan-id*). Multiple entries are separated by (-) (hyphen) or (,) (comma).
- You can apply only one VLAN access map to each VLAN.

When entering the **no** form of this command, the *vlan-list* parameter is optional (but the keyword **vlan-list** is required). If you do not enter the *vlan-list* parameter, the VACL is removed from all VLANs where the *map-name* is applied.

Examples This example shows how to apply a VLAN access map on VLANs 7 through 9:

```
Switch(config)# vlan filter ganymede vlan-list 7-9
Switch(config)#
```

vlan internal allocation policy

Use the **vlan internal allocation policy** command to configure the internal VLAN allocation scheme. Use the **no** form of this command to return to the default setting.

vlan internal allocation policy { ascending | descending }

no vlan internal allocation policy

Syntax Description

ascending	Allocates internal VLANs from 1006 to 4094.
descending	Allocates internal VLANs from 4094 to 1006.

Defaults

The default is the ascending allocation scheme.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

You can configure internal VLAN allocation to be from 1006 and up or from 4094 and down.

Internal VLANs and user-configured VLANs share the 1006 to 4094 VLAN spaces. A “first come, first served” policy is used in allocating these spaces.

The **vlan internal allocation policy** command allows you to configure the allocation direction of the internal VLAN.

During system bootup, internal VLANs required for features in the startup-config file are allocated first. User-configured VLANs in the startup-config file are configured next. If you configure a VLAN that conflicts with an existing internal VLAN, the VLAN you configured is put into a nonoperational status until the internal VLAN is freed and becomes available.

After you enter the **write mem** command and the system reloads, the reconfigured allocation scheme is used by the port manager.

Examples

This example shows how to configure VLANs in a descending order as the internal VLAN allocation policy:

```
Switch(config)# vlan internal allocation policy descending
Switch(config)#
```

Related Commands

[show vlan internal usage](#)

vmps reconfirm (global configuration)

To change the reconfirmation interval for the VLAN Query Protocol (VQP) client, use the **vmps reconfirm** command. To return to the default setting, use the **no** form of this command.

vmps reconfirm *interval*

no vmps reconfirm

Syntax Description	<i>interval</i>	Queries to the VLAN Membership Policy Server (VMPS) to reconfirm dynamic VLAN assignments; valid values are from 1 to 120 minutes.
---------------------------	-----------------	--

Defaults	The reconfirmation interval is 60 minutes.
-----------------	--

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

Command History	<table border="1"> <thead> <tr> <th style="border: none;">Release</th> <th style="border: none;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border: none;">12.1(13)EW</td> <td style="border: none;">Support for this command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Release	Modification				
12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.				

Examples	This example shows how to set the VQP client to reconfirm dynamic VLAN entries every 20 minutes:
-----------------	--

```
Switch(config)# vmps reconfirm 20
Switch(config)#
```

You can verify your setting by entering the **show vmps** command and examining information in the Reconfirm Interval row.

Related Commands	show vmps vmps reconfirm (privileged EXEC)
-------------------------	---

vmps reconfirm (privileged EXEC)

To immediately send VLAN Query Protocol (VQP) queries to reconfirm all dynamic VLAN assignments with the VLAN Membership Policy Server (VMPS), use the **vmps reconfirm** command.

vmps reconfirm

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines You can verify your setting by entering the **show vmps** 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.

Examples This example shows how to immediately send VQP queries to the VMPS:

```
Switch# vmps reconfirm
Switch#
```

Related Commands [show vmps](#)
[vmps reconfirm \(global configuration\)](#)

vmps retry

To configure the per-server retry count for the VLAN Query Protocol (VQP) client, use the **vmps retry** command. To return to the default setting, use the **no** form of this command.

vmps retry *count*

no vmps retry

Syntax Description	<i>count</i> Number of attempts to contact the VLAN Membership Policy Server (VMPS) by the client before querying the next server in the list; valid values are from 1 to 10.				
Defaults	The retry count is 3.				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Release</th> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border-bottom: 1px solid black;">12.1(13)EW</td> <td style="border-bottom: 1px solid black;">Support for this command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Release	Modification				
12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.				
Usage Guidelines	You can verify your setting by entering the show vmps command and examining information in the Server Retry Count row.				
Examples	<p>This example shows how to set the retry count to 7:</p> <pre>Switch(config)# vmps retry 7</pre>				
Related Commands	show vmps				

vmmps server

To configure the primary VLAN Membership Policy Server (VMPS) and up to three secondary servers, use the **vmmps server** command. To remove a VMPS server, use the **no** form of this command.

vmmps server *ipaddress* [**primary**]

no vmmps server *ipaddress*

Syntax Description		
	<i>ipaddress</i>	IP address or host name of the primary or secondary VMPS servers. If you specify a host name, 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(4)EA1	This command was first introduced.

Usage Guidelines

The first server entered is automatically selected as the primary server whether or not **primary** is entered. You can override the first server address 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 that is 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.

You can verify your setting by entering the **show vmmps** command and examining information in the VMPS Domain Server row.

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)# vmps server 191.10.49.20 primary
Switch(config)# vmps server 191.10.49.21
Switch(config)# vmps server 191.10.49.22
Switch(config)#
```

This example shows how to delete the server with IP address 191.10.49.21:

```
Switch(config)# no vmps server 191.10.49.21
Switch(config)#
```

Related Commands [show vmps](#)

vtp (global configuration mode)

To modify the name of a VTP configuration storage file, use the **vtp** command. To clear a filename, use the **no** form of this command.

```
vtp {{file filename} | {if-id name}}
```

```
no vtp {file filename} | {if-id name}}
```

Syntax Description	file filename	Specifies the IFS file where VTP configuration will be stored.
	if-id name	Specifies the name of the interface providing the VTP updater ID for this device, where the if-id name is an ASCII string limited to 255 characters.

Defaults	Disabled
----------	----------

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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines You cannot use the **vtp file** command to load a new database. You can use it only to rename the file in which the existing database is stored.

You can use the **vtp if-id** command to specify the name of the interface providing the VTP updater ID for this device. The VTP updater is the device that adds, deletes, or modifies VLANs to a network, and triggers a VTP updater to inform the rest of the system of the changes.

Examples This example shows how to specify the IFS file system file where VTP configuration is stored:

```
Switch(config)# vtp file vtpconfig
Setting device to store VLAN database at filename vtpconfig.
Switch(config)#
```

This example shows how to specify the name of the interface providing the VTP updater ID:

```
Switch(config)# vtp if-id fastethernet
Switch(config)#
```

Related Commands	show vtp
------------------	--------------------------

vtp client

To place a device in VTP client mode, use the **vtp client** command. To return to VTP server mode, use the **no vtp client** form of this command.

vtp client

no vtp client

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes VLAN configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines 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.

The **vtp server** command is the functional equivalent of **no vtp client** except that it does not return an error if the device is not in client mode.

Examples This example shows how to place the device in VTP client mode:

```
Switch(vlan-config)# vtp client
Switch(vlan-config)#
```

Related Commands [show vtp](#)
[vtp \(global configuration mode\)](#)

vtp domain

To configure the administrative domain name for a device, use the **vtp domain** command.

vtp domain *domain-name*

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

Defaults	This command has no default settings.
-----------------	---------------------------------------

Command Modes	VLAN configuration
----------------------	--------------------

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	<p>When you define the <i>domain-name</i>, the domain name is case sensitive and can be from 1 to 32 characters. You must set a domain name before you can transmit any VTP advertisements.</p> <p>Even if you do not set a domain name, the device will leave the no-management-domain state upon receiving the first VTP summary packet on any port that is currently trunking.</p> <p>If the device receives its domain from a summary packet, it resets its configuration revision number to zero. Once the device leaves the no-management-domain state, it can never be configured to reenter the number except by cleaning NVRAM and reloading.</p>
-------------------------	--

Examples	This example shows how to set the devices administrative domain:
-----------------	--

```
Switch(vlan-config)# vtp domain DomainChandon
Switch(vlan-config)#
```

Related Commands	<p>show vtp</p> <p>vtp (global configuration mode)</p>
-------------------------	--

vtp password

To create a VTP domain password, use the **vtp password** command. To delete the password, use the **no** form of this command.

vtp password *password-value*

no vtp password

Syntax Description	<i>password-value</i> An ASCII string, from 1 to 32 characters, identifying the administrative domain for the device.
---------------------------	---

Defaults	Disabled
-----------------	----------

Command Modes	VLAN configuration
----------------------	--------------------

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to create a VTP domain password:

```
Switch(vlan-config)# vtp password DomainChandon
Switch(vlan-config)#
```

This example shows how to delete the VTP domain password:

```
Switch(vlan-config)# no vtp password
Clearing device VLAN database password.
Switch(vlan-config)#
```

Related Commands	show vtp vtp (global configuration mode)
-------------------------	---

vtp pruning

To enable pruning in the VLAN database, use the **vtp pruning** command. To disable pruning in the VLAN database, use the **no** form of this command.

vtp pruning

no vtp pruning

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes VLAN configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if there are no stations belonging to that VLAN.

Examples This example shows how to enable pruning in the VLAN database:

```
Switch(vlan-config)# vtp pruning
Pruning switched ON
Switch(vlan-config)#
```

This example shows how to disable pruning in the VLAN database:

```
Switch(vlan-config)# no vtp pruning
Pruning switched OFF
Switch(vlan-config)#
```

Related Commands [show vtp](#)
[vtp \(global configuration mode\)](#)

vtp server

To place the device in VTP server mode, use the **vtp server** command.

vtp server

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes VLAN configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

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.

You can set VTP to either server or client mode only when you disable dynamic VLAN creation.

If the receiving switch is in server mode, the configuration is not changed.

The **vtp server** command is the functional equivalent of **no vtp client**, except that it does not return an error if the device is not in client mode.

Examples This example shows how to place the device in VTP server mode:

```
Switch(vlan-config)# vtp server
Switch(vlan-config)#
```

Related Commands

- [show vtp](#)
- [vtp \(global configuration mode\)](#)

vtp transparent

To place a device in VTP transparent mode, use the **vtp transparent** command. To return to VTP server mode, use the **no** form of this command.

vtp transparent

no vtp transparent

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes VLAN configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines The **vtp transparent** command disables VTP from the domain but does not remove the domain from the switch.

If the receiving switch is in transparent mode, the configuration is not changed. Switches in transparent mode do not participate in VTP. If you make VTP or VLAN configuration changes on a switch in transparent mode, the changes are not propagated to the other switches in the network.

The **vtp server** command is similar to the **no vtp transparent** command, except that it does not return an error if the device is not in transparent mode.

Examples This example shows how to place the device in VTP transparent mode:

```
Switch(vlan-config)# vtp transparent
Switch(vlan-config)#
```

This example shows how to return the device to VTP server mode:

```
Switch(vlan-config)# no vtp transparent
Switch(vlan-config)#
```

Related Commands [show vtp](#)
[vtp \(global configuration mode\)](#)

vtp v2-mode

To enable version 2 mode, use the **vtp v2-mode** command. To disable version 2 mode, use the **no** form of this command.

vtp v2-mode

no vtp v2-mode

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes VLAN configuration

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines All switches in a VTP domain must run the same version of VTP. VTP version 1 and VTP version2 do not operate on switches in the same VTP domain.

If all switches in a domain are VTP version 2-capable, you only need to enable VTP version 2 on one switch; the version number is then propagated to the other version 2-capable switches in the VTP domain.

If you toggle the version 2 mode, parameters of certain default VLANs will be modified.

Examples This example shows how to enable version 2 mode in the VLAN database:

```
Switch(vlan-config)# vtp v2-mode
Switch(vlan-config)#
```

This example shows how to disable version 2 mode in the VLAN database:

```
Switch(vlan-config)# no vtp v2-mode
Switch(vlan-config)#
```

Related Commands [show vtp](#)
[vtp \(global configuration mode\)](#)



Symbols

- \$ matches the end of a string [1-7](#)
- () in commands [1-10](#)
- * matches 0 or more sequences of a pattern [1-7](#)
- + matches 1 or more sequences of a pattern [1-7](#)
- . matches any single character [1-7](#)
- ? command [1-1](#)
- ? matches 0 or 1 occurrence of a pattern [1-7](#)
- ^ matches the beginning of a string [1-7](#)
- _ matches a comma (,), left brace ({), left parenthesis [1-7](#)
- “ [1-10](#)

Numerics

- 802.1Q trunk ports and native VLANs [2-501](#)
- 802.1Q tunnel ports
 - configuring [2-462](#)
- 802.1s Multiple Spanning Tree
 - see MST
- 802.1x Port Based Authentication
 - allowing multiple hosts on a port [2-85](#)
 - debugging 802.1x Port Based Authentication [2-48](#)
 - displaying port based authentication [2-255](#)
 - enabling accounting for authentication sessions [2-3](#)
 - enabling authentication on the system [2-90](#)
 - enabling guest VLAN [2-81](#)
 - enabling manual control of auth state [2-86](#)
 - enabling periodic re-authentication of the client [2-89](#)
 - initializing re-authentication of dot1x ports [2-88](#)
 - initializing state machines [2-82](#)
 - receive session termination message upon reboot [2-4](#)
 - setting maximum number for EAP requests [2-84](#)

A

- abbreviating commands
 - context-sensitive help [1-1](#)
- Access Gateway Module
 - connecting to a module [2-9](#)
 - connecting to a remote module [2-230](#)
 - connecting to a specific remote module [2-236](#)
- access-group
 - displaying mac interface [2-335](#)
 - show mode interface [2-239](#)
- access groups
 - IP [2-5](#)
- access lists
 - clearing an access template [2-25](#)
 - defining ARP [2-8](#)
 - displaying ARP information [2-240](#)
 - See also ACLs, MAC ACLs, and VACLs
- access maps
 - applying with VLAN filter [2-502](#)
- ACLs
 - access-group mode [2-5](#)
 - displaying mac access-group interface [2-335](#)
 - using ACL naming conventions for MAC ACLs [2-163](#)
- action clause
 - specifying drop or forward action in a VACL [2-6](#)
- adjacency
 - debugging the adjacency table [2-42](#)
 - disabling the debug facility [2-42](#)
 - displaying IPC table entries [2-42](#)
- aggregate policer
 - displaying information [2-368](#)

aging time
 displaying MAC address aging time [2-338](#)
 MAC address table [2-166](#)

alarms
 displaying operational status [2-258](#)

alternation
 description [1-9](#)

anchoring
 description [1-10](#)

ARP
 access list, displaying detailed information [2-240](#)
 defining access-lists [2-8](#)

ARP inspection
 enforce certain types of checking [2-118](#)

ARP packet
 deny based on DHCP bindings [2-78](#)
 permit based on DHCP bindings [2-190](#)

authentication
 setting username [2-492](#)
 using an MD5-type encryption method [2-492](#)
 verifying MD5 signature [2-493](#)
 verifying the checksum for Flash memory [2-493](#)

authorization state
 enabling manual control [2-86](#)

authorization state of a controlled port [2-86](#)

auto-QoS
 configuring for VoIP [2-10](#)
 displaying configuration [2-241](#)

B

baby giants
 displaying the system MTU setting [2-393](#)
 setting the maximum Layer 2 payload size [2-477](#)

BackboneFast
 displaying debugging messages [2-67](#)
 displaying spanning tree status [2-384](#)
 enabling debugging [2-67](#)

bindings
 store for DHCP snooping [2-126](#)

BOOT environment variable
 displaying information [2-245](#)

bootflash
 displaying information [2-243](#)

BPDUs
 debugging spanning tree activities [2-66](#)

bridge protocol data units
 See BPDUs

broadcast suppression level
 configuring [2-454, 2-456](#)
 enabling [2-454, 2-456](#)

C

Catalyst 4507R [2-200](#)
 power redundancy mode [2-202](#)

CDP
 configuring tunneling encapsulation rate [2-160](#)
 enabling protocol tunneling for [2-157](#)
 set drop threshold for [2-159](#)

CEF
 displaying next-hop information [2-299](#)
 displaying VLAN configuration information [2-299](#)

cisco-desktop
 macro apply [2-172](#)

Cisco Express Forwarding
 See CEF

cisco-phone
 macro apply [2-174](#)

cisco-router
 macro apply [2-176](#)

cisco-switch
 macro apply [2-178](#)

clear commands
 clearing Gigabit Ethernet interfaces [2-23](#)
 clearing IGMP group cache entries [2-30](#)
 clearing interface counters [2-20](#)

- clearing IP access lists [2-25, 2-26](#)
 - clearing IP ARP inspection statistics VLAN [2-27](#)
 - clearing IP DHCP snooping database [2-28](#)
 - clearing IP DHCP snooping database statistics [2-29](#)
 - clearing MFIB counters and routes [2-33](#)
 - clearing MFIB fastdrop entries [2-34](#)
 - clearing PAgP channel information [2-37](#)
 - clearing QoS aggregate counters [2-39](#)
 - clearing VLAN interfaces [2-24](#)
 - CLI string search
 - anchoring [1-10](#)
 - expressions [1-7](#)
 - filtering [1-6](#)
 - multiple-character patterns [1-8](#)
 - multipliers [1-9](#)
 - parentheses for recall [1-10](#)
 - searching outputs [1-6](#)
 - single-character patterns [1-7](#)
 - using [1-6](#)
 - command modes
 - accessing privileged EXEC mode [1-4](#)
 - exiting [1-4](#)
 - understanding user EXEC and configuration modes [1-4](#)
 - condition interface
 - debugging interface-related activities [2-44](#)
 - condition vlan
 - debugging VLAN output [2-47](#)
 - configuration, saving [1-11](#)
 - configuring
 - root as secondary [2-437](#)
 - configuring a SPAN session to monitor
 - limit SPAN source traffic [2-182](#)
 - configuring forward delay [2-433](#)
 - configuring root as primary [2-437](#)
 - CoS
 - assigning to Layer 2 protocol packets [2-158](#)
 - CoS QoS default
 - defining value on an interface [2-215](#)
 - Cost of Service
 - See QoS CoS
 - counters
 - clearing interface counters [2-20](#)
-
- D
 - DAI
 - clear statistics [2-27](#)
 - DBL
 - displaying qos dbl [2-369](#)
 - enabling DBL globally on the switch [2-216](#)
 - debug commands
 - debugging backup events [2-43](#)
 - debugging DHCP snooping events [2-53](#)
 - debugging DHCP snooping messages [2-54](#)
 - debugging EtherChannel/PAgP/shim [2-49](#)
 - debugging IPC activity [2-52](#)
 - debugging IP DHCP snooping security messages [2-55](#)
 - debugging NVRAM activities [2-58](#)
 - debugging PAgP activities [2-59](#)
 - debugging port manager activities [2-62](#)
 - debugging software MAC filter updates [2-65](#)
 - debugging spanning tree activities [2-66](#)
 - debugging spanning tree backbonefast [2-67](#)
 - debugging spanning tree UplinkFast [2-70](#)
 - debugging supervisor redundancy [2-64](#)
 - debugging VLAN manager activities [2-71](#)
 - displaying monitor activity [2-57](#)
 - displaying the adjacency table [2-42](#)
 - enabling debug dot1x [2-48](#)
 - enabling debugging messages for ISL VLAN IDs [2-73](#)
 - enabling debugging messages for VTP [2-74](#)
 - enabling debugging of UDLD activity [2-75](#)
 - enabling switch shim debugging [2-68](#)
 - enabling VLAN manager file system error tests [2-72](#)
 - limiting debugging output for VLANs [2-47](#)
 - limiting interface debugging output [2-44](#)

- limiting output for debugging standby state changes [2-45](#)
 - shortcut to the debug condition interface [2-51](#)
 - debugging
 - activity monitoring [2-57](#)
 - DHCP snooping events [2-53](#)
 - DHCP snooping packets [2-54](#)
 - IPC activities [2-52](#)
 - IP DHCP snooping security packets [2-55](#)
 - NVRAM activities [2-58](#)
 - PAgP activities [2-59](#)
 - PAgP shim [2-49](#)
 - PM activities [2-62](#)
 - SMF address insertions and deletions [2-65](#)
 - spanning tree BackboneFast events [2-67](#)
 - spanning tree switch shim [2-68](#)
 - spanning tree UplinkFast events [2-70](#)
 - VLAN manager activities [2-71](#)
 - VLAN manager IOS file system error tests [2-72](#)
 - VTP protocol debug messages [2-74](#)
 - debug spanning tree switch [2-68](#)
 - debug sw-vlan vtp [2-74](#)
 - default CoS value [2-215](#)
 - default form of a command, using [1-6](#)
 - defining egress DSCP-to-CoS mapping [2-220](#)
 - DHCP
 - clearing database statistics [2-29](#)
 - DHCP bindings
 - configuring bindings [2-125](#)
 - deny ARP packet based on matches [2-78](#)
 - permit ARP packet based on matches [2-190](#)
 - DHCP snooping
 - clearing database [2-28](#)
 - displaying [2-300](#)
 - displaying binding table [2-301](#)
 - displaying status of DHCP database [2-304](#)
 - displaying status of error detection [2-261](#)
 - enabling DHCP globally [2-124](#)
 - enabling IP source guard [2-155](#)
 - enabling on a VLAN [2-131](#)
 - enabling option 82 [2-128](#)
 - enabling rate limiting on an interface [2-129](#)
 - enabling trust on an interface [2-130](#)
 - establishing binding configuration [2-125](#)
 - renew binding database [2-232](#)
 - store generated bindings [2-126](#)
 - diagnostic test
 - display module-based results [2-247](#)
 - displaying error disable recovery [2-262](#)
 - displaying inline power status [2-363](#)
 - displaying monitoring activity [2-57](#)
 - displaying SEEPROM information
 - GBIC [2-269](#)
 - displaying SPAN session information [2-392, 2-455](#)
 - document conventions [xvi](#)
 - document organization [xv](#)
 - DOS attack
 - protecting system's resources [2-113](#)
 - drop threshold, Layer 2 protocol tunneling [2-159](#)
 - DSCP rewrite for IP packets
 - enable [2-223](#)
 - duplex mode
 - configuring autonegotiation on an interface [2-93](#)
 - configuring full duplex on an interface [2-93](#)
 - configuring half duplex on an interface [2-93](#)
 - dynamic ARP inspection
 - preventing [2-113](#)
 - Dynamic Buffer Limiting
 - See DBL
 - Dynamic Host Configuration Protocol
 - See DHCP
-
- ## E
- EAP
 - restarting authentication process [2-84](#)
 - enabling
 - debugging for UDLD [2-75](#)

- voice VLANs [2-457](#)
- environmental
 - alarms [2-258](#)
 - displaying information [2-258](#)
 - status [2-258](#)
 - temperature [2-258](#)
- error disable detection
 - enabling error disable detection [2-95](#)
- error-disabled state
 - displaying [2-285](#)
- error disable recovery
 - configuring recovery mechanism variables [2-97](#)
 - displaying recovery timer information [2-262](#)
 - enabling ARP inspection timeout [2-97](#)
 - specifying recovery cause [2-97](#)
- EtherChannel
 - assigning interfaces to EtherChannel groups [2-14](#)
 - debugging EtherChannel [2-49](#)
 - debugging PAgP shim [2-49](#)
 - debugging spanning tree activities [2-66](#)
 - displaying information for a channel [2-263](#)
 - removing interfaces from EtherChannel groups [2-14](#)
- EtherChannel guard
 - detecting STP misconfiguration [2-424](#)
- Explicit Host Tracking
 - clearing the database [2-32](#)
 - displaying host membership [2-312](#)
 - enabling per-VLAN [2-142](#)
- expressions
 - matching multiple expression occurrences [1-9](#)
 - multiple-character patterns [1-8](#)
 - multiplying pattern occurrence [1-10](#)
 - single-character patterns [1-7](#)
- Extensible Authentication Protocol
 - See EAP

F

- field replaceable unit (FRU)
 - displaying status information [2-258](#)
- Flash memory file system
 - displaying file system information [2-243](#)
 - verifying checksum [2-493](#)
- flow control
 - configuring a gigabit interface for pause frames [2-100](#)
 - displaying per-interface statistics for flow control [2-267](#)

G

- GBIC
 - displaying SEEPROM information [2-269](#)
- Gigabit Ethernet interface
 - clearing the hardware logic [2-23](#)
- global configuration mode
 - using [1-5](#)

H

- hardware module
 - resetting a module by toggling the power [2-103](#)
- host membership on an interface
 - displaying information [2-312](#)
- hot standby protocol
 - debugging [2-45](#)
 - disabling debugging [2-45](#)
 - limiting output [2-45](#)

I

- IDPROMs
 - displaying SEEPROM information
 - chassis [2-269](#)
 - clock module [2-269](#)
 - fan trays [2-269](#)

- module [2-269](#)
 - mux buffer [2-269](#)
 - power supplies [2-269](#)
 - supervisor engine [2-269](#)
- ifIndex persistence
 - clearing SNMP ifIndex commands [2-413](#)
 - compress SNMP ifIndex table format [2-418](#)
 - disabling globally [2-417](#)
 - disabling on an interface [2-414](#)
 - enabling globally [2-417](#)
 - enabling on an interface [2-414](#)
- IGMP
 - applying filters for host joining on Layer 2 interfaces [2-133](#)
 - clearing IGMP group cache entries [2-30](#)
 - configuring frequency for IGMP host-query messages [2-136](#)
 - creating an IGMP profile [2-135](#)
 - displaying IGMP interface configuration information [2-306](#)
 - displaying profiles [2-307](#)
 - setting maximum group numbers [2-134](#)
- IGMP profiles
 - displaying [2-307](#)
- IGMP snooping
 - clearing the EHT database [2-32](#)
 - configuring a Layer 2 interface as a group member [2-146](#)
 - configuring a Layer 2 interface as a multicast router [2-144](#)
 - configuring a static VLAN interface [2-146](#)
 - displaying host membership [2-312](#)
 - displaying multicast information [2-314](#)
 - displaying VLAN information [2-308, 2-315](#)
 - enabling [2-137](#)
 - enabling immediate-leave processing [2-143](#)
 - enabling on a VLAN [2-141](#)
 - enabling per-VLAN Explicit Host Tracking [2-142](#)
- informs
 - enabling [2-415](#)
- inline power
 - displaying inline power status [2-363](#)
- inspection log
 - clearing log buffer [2-26](#)
- interface
 - displaying suppressed multicast bytes [2-279](#)
- interface capabilities
 - displaying [2-276](#)
- interface configuration mode
 - summary [1-5](#)
- interface link
 - display cable disconnect time [2-282](#)
- interfaces
 - configuring dot1q tunnel ports [2-462](#)
 - creating an interface-range macro [2-77](#)
 - debugging output of interface related activities [2-44](#)
 - displaying description [2-281](#)
 - displaying error-disabled state [2-285](#)
 - displaying information when tunneling is enabled [2-329](#)
 - displaying status [2-281](#)
 - displaying traffic for a specific interface [2-274](#)
 - executing a command on multiple ports in a range [2-108](#)
 - setting a CoS value for Layer 2 packets [2-158](#)
 - setting drop threshold for Layer 2 packets [2-159](#)
 - setting the interface type [2-462](#)
- interface speed
 - configuring interface speed [2-451](#)
- interface transceiver
 - displaying diagnostic data [2-288](#)
- internal VLAN allocation
 - configuring [2-503](#)
 - default setting [2-503](#)
 - displaying allocation information [2-403](#)
- Internet Group Management Protocol
 - See IGMP
- IP ARP
 - applying ARP ACL to VLAN [2-111](#)
 - clearing inspection statistics [2-27](#)
 - clearing status of log buffer [2-26](#)

- controlling packet logging [2-121](#)
- enabling dynamic inspection [2-120](#)
- limit rate of incoming requests [2-113](#)
- set per-port config trust state [2-117](#)
- showing status of dynamic ARP inspection [2-295](#)
- showing status of log buffer [2-298](#)

IPC

- debugging IPC activities [2-52](#)

IP DHCP Snooping

- See DHCP snooping

IP header validation

- disabling [2-154](#)
- enabling [2-154](#)

IP multicast

- displaying multicast routing table information [2-319](#)

IP packets

- enable DSCP rewrite [2-223](#)

IP phone and standard desktop

- enabling Cisco-recommended features [2-174](#)

IP source binding

- adding or deleting [2-151](#)
- displaying bindingstaggering [2-324](#)

IP source guard

- debugging messages [2-55](#)
- displaying configuration and filters [2-325](#)
- enabling on DHCP snooping [2-155](#)

J

Jumbo frames

- enabling jumbo frames [2-186](#)

L

l2protocol-tunnel cos command [2-158](#)

LACP

- deselecting channeling protocol [2-16](#)
- enabling LACP on an interface [2-16](#)

- setting channeling protocol [2-16](#)

Layer 2

- displaying ACL configuration [2-335](#)

Layer 2 interface type

- specifying a nontrunking, nontagged single VLAN interface [2-462](#)
- specifying a trunking VLAN interface [2-462](#)

Layer 2 protocol ports

- displaying [2-329](#)

Layer 2 protocol tunneling error recovery [2-160](#)

Layer 2 switching

- enabling voice VLANs [2-457](#)
- modifying switching characteristics [2-457](#)

Layer 2 traceroute

- IP addresses [2-481](#)

Layer 3 switching

- displaying port status [2-286](#)
- displaying status of native VLAN tagging [2-286](#)

log buffer

- show status [2-298](#)

logging

- ip arp inspection vlan command [2-121](#)

M

MAC Access Control Lists

- See MAC ACLs

MAC ACLs

- defining extended MAC access list [2-163](#)
- displaying MAC ACL information [2-400](#)
- naming an ACL [2-163](#)

MAC address filtering

- configuring [2-170](#)
- disabling [2-170](#)
- enabling [2-170](#)

MAC address table

- adding static entries [2-180](#)
- clearing dynamic entries [2-36](#)
- configuring aging time [2-166](#)

- displaying dynamic table entry information [2-340](#)
- displaying entry count [2-339](#)
- displaying information [2-336](#)
- displaying interface-based information [2-342](#)
- displaying multicast information [2-344](#)
- displaying protocol-based information [2-346](#)
- displaying static table entry information [2-348](#)
- displaying the MAC address aging time [2-338](#)
- displaying VLAN-based information [2-350](#)
- learning in the protocol buckets [2-167](#)
- removing static entries [2-180](#)
- MAC address tables
 - adding static entries [2-170](#)
 - deleting secure or specific addresses [2-38](#)
 - disabling IGMP snooping on static MAC addresses [2-170](#)
 - removing static entries [2-170](#)
- mac-address-table static [2-170](#)
- MAC address unicast filtering
 - dropping unicast traffic [2-170](#)
- macro keywords
 - help strings [2-2](#)
- mapping secondary VLANs to MST instance [2-207](#)
- mapping VLAN(s) to an MST instance [2-104](#)
- match subcommand
 - accessing [2-18](#)
- maximum transmission unit (MTU)
 - displaying the system MTU setting [2-393](#)
 - setting the maximum Layer 2 payload size [2-477](#)
- MD5
 - verifying MD5 signature [2-493](#)
- message digest 5
 - See MD5
- MFIB
 - clearing ip mfib counters [2-33](#)
 - clearing ip mfib fastdrop [2-34](#)
 - displaying all active MFIB routes [2-316](#)
 - displaying MFIB fastdrop table entries [2-318](#)
 - enabling IP MFIB fastdrops [2-148](#)
- modes
 - access-group [2-5](#)
 - show access-group interface [2-239](#)
 - switching between PVST+, MST, and Rapid PVST [2-429](#)
 - See also command modes
- module password clearing [2-22](#)
- module reset
 - resetting a module by toggling the power [2-103](#)
- More-- prompt
 - filter [1-6](#)
 - search [1-7](#)
- MST
 - designating the primary and secondary root [2-437](#)
 - displaying MST protocol information [2-389](#)
 - displaying region configuration information [2-389](#)
 - displaying spanning tree information [2-389](#)
 - entering MST configuration submode [2-431](#)
 - setting configuration revision number [2-234](#)
 - setting path cost and port priority for instances [2-430](#)
 - setting the forward delay timer for all instances [2-433](#)
 - setting the hello-time delay timer for all instances [2-434](#)
 - setting the max-age timer for all instances [2-435](#)
 - setting the MST region name [2-187](#)
 - specifying the maximum number of hops [2-436](#)
 - switching between PVST+ and Rapid PVST [2-429](#)
 - using the MST configuration submode revision command [2-234](#)
 - using the submode name command [2-187](#)
- MTU
 - displaying global MTU settings [2-393](#)
- multicast
 - enabling storm control [2-456](#)
- multicast/unicast packets
 - prevent forwarding [2-461](#)
- Multicast Forwarding Information Base
 - See MFIB
- multiple-character patterns [1-8](#)
- multiple hosts on authorized port [2-85](#)

Multiple Spanning Tree

See MST

N

native VLAN

- controlling tagging of traffic [2-473](#)
- displaying ports eligible for native tagging [2-402](#)
- displaying ports eligible for tagging [2-402](#)
- enabling tagging on 802.1Q trunk ports [2-501](#)
- specifying the tagging of traffic [2-474](#)

NetFlow

- enabling NetFlow statistics [2-149](#)
- including infer fields in routing statistics [2-149](#)

next-hop

- displaying CEF VLAN information [2-299](#)

no form of a command, using [1-6](#)

NVRAM

- debugging NVRAM activities [2-58](#)

O

output

- pattern searches [1-7](#)

P

packet forwarding

- prevent unknown packets [2-461](#)

packet memory failure

- direct switch action upon detection [2-80](#)

packet memory test

- bootup, displaying results [2-251](#)
- ongoing, displaying results [2-253](#)

PACL

- access-group mode [2-5](#)

paging prompt

- see --More-- prompt

PAGP

- clearing port channel information [2-37](#)
- debugging PAGP activity [2-59](#)
- deselecting channeling protocol [2-16](#)
- displaying port channel information [2-356](#)
- hot standby mode
 - returning to defaults [2-189](#)
 - selecting ports [2-189](#)
- input interface of incoming packets
 - learning [2-188](#)
 - returning to defaults [2-188](#)
- setting channeling protocol [2-16](#)

parentheses [1-10](#)

password

- clearing on an intelligent line module [2-22](#)
- establishing enhanced password security [2-492](#)
- setting username [2-492](#)

PBR

- displaying route maps [xvi](#)
- redistributing route maps [xvi](#)

PM activities

- debugging [2-62](#)
- disabling debugging [2-62](#)

Policy Based Routing

See PBR

Port Aggregation Protocol

See PAGP

port-based authentication

- displaying debug messages [2-48](#)
- displaying statistics and status [2-255](#)
- enabling 802.1X [2-86](#)
- manual control of authorization state [2-86](#)
- multiple hosts on authorized port [2-85](#)
- periodic re-authentication
 - enabling [2-89](#)
- re-authenticating 802.1X-enabled ports [2-88](#)
- switch-to-client frame-retransmission number [2-84](#)

port channel

- accessing [2-107](#)

- creating [2-107](#)
 - displaying information [2-356](#)
 - load distribution method
 - resetting to defaults [2-194](#)
 - setting [2-194](#)
 - port range
 - executing [2-108](#)
 - port security
 - debugging ports security [2-63](#)
 - deleting secure or specific addresses [2-38](#)
 - enabling [2-464](#)
 - filter source IP and MAC addresses [2-155](#)
 - setting action upon security violation [2-464](#)
 - setting the rate limit for bad packets [2-464](#)
 - sticky port [2-464](#)
 - Port Trust Device
 - displaying [2-370](#)
 - power status
 - displaying inline power [2-363](#)
 - displaying power status [2-363](#)
 - power supply
 - configuring combined and redundant power on the Catalyst 4507R [2-200](#)
 - configuring inline power [2-197](#)
 - configuring power consumption [2-199](#)
 - configuring power redundancy on the Catalyst 4507R [2-202](#)
 - displaying the SEEPROM [2-269](#)
 - setting inline power state [2-196](#)
 - Private VLAN
 - See PVLANS
 - privileged EXEC mode, summary [1-5](#)
 - prompts
 - system [1-5](#)
 - protocol tunneling
 - configuring encapsulation rate [2-160](#)
 - disabling [2-157](#)
 - displaying port information [2-329](#)
 - enabling [2-157](#)
 - setting a CoS value for Layer 2 packets [2-158](#)
 - setting a drop threshold for Layer 2 packets [2-159](#)
 - PVLANS
 - configuring isolated and primary PVLANS [2-203](#)
 - controlling tagging of native VLAN traffic [2-473](#)
 - disabling sticky-ARP [2-152](#)
 - displaying map information for VLAN SVIs [2-284](#)
 - displaying PVLAN information [2-405](#)
 - enabling interface configuration mode [2-462](#)
 - enabling sticky-ARP [2-152](#)
 - mapping VLANs to the same SVI [2-205](#)
 - specifying host ports [2-462](#)
 - specifying promiscuous ports [2-462](#)
 - PVST+
 - switching between PVST and MST [2-429](#)
-
- ## Q
- QoS
 - account Layer 2 encapsulation [2-210](#)
 - attaching a policy-map to an interface [2-235](#)
 - automatic configuration [2-10](#)
 - clearing aggregate counters [2-39](#)
 - configuring a QoS policy map [2-192](#)
 - configuring auto [2-10](#)
 - defining a named aggregate policer [2-212](#)
 - defining default CoS value [2-215](#)
 - defining ingress CoS-to-DSCP mapping [2-219](#)
 - displaying aggregate policer information [2-368](#)
 - displaying auto configuration [2-241](#)
 - displaying class maps information [2-246](#)
 - displaying configuration information [2-241](#)
 - displaying configurations of policies [2-359](#)
 - displaying policy map information [2-358](#)
 - displaying QoS information [2-367](#)
 - displaying QoS map information [2-371](#)
 - enabling global configuration mode [2-208](#)
 - enabling per-VLAN QoS for a Layer 2 interface [2-226](#)
 - enabling QoS on an interface [2-209](#)

- mapping DSCP values to transmit queues [2-220](#)
- mapping egress DSCP-to-CoS [2-220](#)
- mapping the DSCP-to-CoS value [2-220](#)
- setting the mapping of policed DSCP values [2-222](#)
- setting the trust state [2-224](#)

QoS CoS

- configuring for tunneled Layer 2 protocol packets [2-158](#)
- defining default CoS value [2-215](#)

qos dbl [2-216](#)

question command [1-1](#)

queueing information

- displaying [2-370](#)

R

Rapid PVST

- switching between PVST and MST [2-429](#)

re-authenticating 802.1X-enabled ports [2-88](#)

re-authentication

- periodic [2-89](#)

reboots

- restoring bindings across [2-125](#)

redundancy

- accessing the main CPU [2-227](#)
- changing from active to standby supervisor engine [2-228](#)
- displaying information [2-373](#)
- displaying redundancy facility information [2-373](#)
- displaying RF client list [2-373](#)
- displaying RF operational counters [2-373](#)
- displaying RF states [2-373](#)
- enabling automatic synchronization [2-13](#)
- forcing switchover to standby supervisor engine [2-228](#)
- synchronizing the route processor configurations [2-180](#)

related documentation [xv](#)

remote SPAN

- See RSPAN

renew commands

- ip dhcp snooping database [2-232](#)

- resetting PVLAN trunk
 - setting switchport to trunk [2-462](#)

ROM monitor mode

- summary [1-6](#)

root guard

- displaying root inconsistency status [2-384](#)

Route Processor Redundancy

- See redundancy

RSPAN

- converting VLAN to RSPAN VLAN [2-231](#)
- displaying list [2-407](#)

S

saving configuration changes [1-11](#)

secure ports, limitations [2-465](#)

show commands

- filtering parameters [1-7](#)
- searching and filtering [1-6](#)

show dot1x command [2-255](#)

show errdisable detect command [2-261](#)

show interfaces capabilities command [2-276](#)

show interfaces transceiver command [2-288](#)

show ip arp inspection command [2-295](#)

show ip arp inspection log command [2-298](#)

show l2protocol-tunnel command [2-329](#)

show platform commands [1-11](#)

show port security command [2-361](#)

show qos interface command [2-370](#)

show vlan remote-span [2-407](#)

Simple Network Management Protocol

- See SNMP

single-character patterns

- special characters [1-7](#)

slaveslot0

- displaying information on the standby supervisor [2-380](#)

slot0

- displaying information about the system [2-382](#)

- SMF
 - debugging address insertions and deletions [2-65](#)
- SNMP
 - debugging spanning tree activities [2-66](#)
 - ifIndex persistence
 - clearing SNMP ifIndex commands [2-413](#)
 - compress SNMP ifIndex table format [2-418](#)
 - disabling globally [2-417](#)
 - disabling on an interface [2-414](#)
 - enabling globally [2-417](#)
 - enabling on an interface [2-414](#)
 - informs
 - disabling [2-415](#)
 - enabling [2-415](#)
 - traps
 - configuring to send when storm occurs [2-454](#)
 - disabling [2-415](#)
 - enabling [2-415](#)
- software MAC filter
 - See SMF
- SPAN
 - configuring a session to monitor [2-182](#)
- SPAN commands
 - displaying SPAN session information [2-392, 2-455](#)
- SPAN enhancements
 - displaying status [2-354](#)
- spanning-tree mode command [2-429](#)
- Spanning Tree Protocol
 - See STP
- SPAN session
 - displaying session information [2-354](#)
 - specifying encap type [2-182](#)
 - turning off host learning based on ingress packets [2-182](#)
- special characters
 - anchoring, table [1-10](#)
- standard desktop
 - enabling Cisco-recommended features [2-172](#)
- standard desktop and Cisco IP phone
 - enabling Cisco-recommended features [2-174](#)
- sticky-ARP
 - disabling on PVLANS [2-152](#)
 - enabling on PVLANS [2-152](#)
- sticky port
 - deleting [2-38](#)
 - enabling security [2-464](#)
- storm control
 - command [2-454, 2-456](#)
 - configuring for action when storm occurs [2-454](#)
 - disabling suppression mode [2-261](#)
 - displaying settings [2-391](#)
 - enabling [2-454](#)
 - enabling broadcast [2-454, 2-456](#)
 - enabling multicast [2-454, 2-456](#)
 - enabling suppression mode [2-261](#)
 - enabling timer to recover from error disable [2-97](#)
 - enabling unicast [2-454, 2-456](#)
 - multicast, enabling [2-456](#)
 - setting high and low levels [2-454](#)
 - setting suppression level [2-261](#)
- STP
 - configuring link type for a port [2-427](#)
 - configuring tunneling encapsulation rate [2-160](#)
 - debugging all activities [2-66](#)
 - debugging spanning tree activities [2-66](#)
 - debugging spanning tree BackboneFast events [2-67](#)
 - debugging spanning tree UplinkFast [2-70](#)
 - detecting misconfiguration [2-424](#)
 - displaying active interfaces only [2-384](#)
 - displaying BackboneFast status [2-384](#)
 - displaying bridge status and configuration [2-384](#)
 - displaying default path cost method [2-384](#)
 - displaying spanning tree debug messages [2-66](#)
 - displaying status information [2-384](#)
 - displaying status per VLAN [2-384](#)
 - displaying summary of interface information [2-384](#)
 - displaying UplinkFast status [2-384](#)
 - enabling BPDU filtering by default on all PortFast ports [2-442](#)

- enabling BPDU filtering on an interface [2-420](#)
- enabling BPDU guard by default on all PortFast ports [2-444](#)
- enabling BPDU guard on an interface [2-422](#)
- enabling extended system ID [2-425](#)
- enabling loop guard as a default on all ports [2-428](#)
- enabling PortFast by default on all access ports [2-445](#)
- enabling PortFast mode [2-440](#)
- enabling protocol tunneling for [2-157](#)
- enabling root guard [2-426](#)
- enabling spanning tree BackboneFast [2-419](#)
- enabling spanning tree on a per VLAN basis [2-449](#)
- enabling spanning tree UplinkFast [2-447](#)
- setting an interface priority [2-446](#)
- setting drop threshold for [2-159](#)
- setting pathcost [2-423](#)
- setting the default pathcost calculation method [2-439](#)
- subinterface configuration mode, summary [1-6](#)
- SVI
 - creating a Layer 3 interface on a VLAN [2-110](#)
- switchport [2-474](#)
- switchport block command [2-461](#)
- switchport interfaces
 - displaying status of Layer 3 port [2-286](#)
 - displaying status of native VLAN tagging [2-286](#)
- switchport mode command [2-462](#)
- switchport port-security aging command [2-468](#)
- switchport port-security command [2-464](#)
- switch shim
 - debugging [2-68](#)
 - disabling debugging [2-68](#)
- switch to router connection
 - enabling Cisco-recommended features [2-176](#)
- switch to switch connection
 - enabling Cisco-recommended features [2-178](#)
- switch virtual interface
 - See SVI
- sw-vlan [2-71](#)
- system prompts [1-5](#)

T

- Tab key
 - command completion [1-1](#)
- tables
 - characters with special meaning [1-7](#)
 - mac access-list extended subcommands [2-163](#)
 - match syntax description [2-19](#)
 - multipliers [1-9](#)
 - relationship between duplex and speed commands [2-452](#)
 - show vlan command output fields [2-405](#)
 - show vtp command output fields [2-410](#)
 - special characters [1-9](#)
 - special characters used for anchoring [1-10](#)
 - speed command options [2-451](#)
- TAC
 - displaying information useful to TAC [2-394](#)
- TCAM
 - debugging spanning tree activities [2-66](#)
- temperature readings
 - displaying information [2-258](#)
- timer information [2-262](#)
- traffic shaping
 - enable on an interface [2-237](#)
- traps, enabling [2-415](#)
- trunk encapsulation
 - setting format [2-474](#)
- trunk interfaces
 - displaying trunk interfaces information [2-293](#)
- trust state
 - setting [2-117](#)
- tunnel ports
 - displaying information about Layer 2 protocol [2-329](#)
- TX queues
 - allocating bandwidth [2-484](#)
 - returning to default values [2-484](#)
 - setting priority to high [2-484](#)
 - specifying burst size [2-484](#)

specifying traffic rate [2-484](#)

U

UDLD

enabling by default on all fiber interfaces [2-486](#)
 enabling on an individual interface [2-488](#)
 preventing a fiber interface from being enabled [2-488](#)
 resetting all shutdown ports [2-490](#)
 setting the message timer [2-486](#)

Unidirectional Link Detection

See UDLD

unknown multicast traffic, preventing [2-461](#)

unknown unicast traffic, preventing [2-461](#)

user EXEC mode, summary [1-5](#)

username

setting password and privilege level [2-492](#)

V

VACLs

access-group mode [2-5](#)
 applying VLAN access maps [2-502](#)
 displaying VLAN access map information [2-400](#)
 specifying an action in a VLAN access map [2-6](#)
 specifying the match clause for a VLAN access-map sequence [2-181](#)
 using a VLAN filter [2-502](#)

VLAN

applying an ARP ACL [2-111](#)
 configuring [2-495](#)
 converting to RSPAN VLAN [2-231](#)
 displaying CEF information [2-299](#)
 displaying CEF next-hop information [2-299](#)
 displaying information on switch interfaces [2-308](#)
 displaying information on VLAN switch interfaces [2-315](#)
 displaying information sorted by group IP address [2-308](#)

displaying IP address and version information [2-308](#)

displaying Layer 2 VLAN information [2-397](#)

displaying statistical information [2-352](#)

displaying VLAN information [2-399](#)

enabling dynamic ARP inspection [2-120](#)

enabling Explicit Host Tracking [2-142](#)

enabling guest per-port [2-81](#)

entering VLAN configuration mode [2-499](#)

native frames

enabling tagging on all 802.1Q trunk ports [2-501](#)

pruning the list for VTP [2-474](#)

setting the list of allowed [2-474](#)

VLAN Access Control Lists

See VACLs

VLAN access map

See VACLs

VLAN database

resetting [2-233](#)

VLAN debugging

limiting output [2-47](#)

VLAN manager

debugging [2-71](#)

disabling debugging [2-71](#)

IOS file system error tests

debugging [2-72](#)

disabling debugging [2-72](#)

VLAN Query Protocol

See VQP

VLAN query protocol (VQPC)

debugging [2-76](#)

VLANs

clearing

counters [2-40](#)

clearing hardware logic [2-24](#)

configuring

internal allocation scheme [2-503](#)

displaying

internal VLAN allocation information [2-403](#)

RSPAN VLANs [2-407](#)

entering VLAN configuration mode [2-499](#)

VMPS

configuring servers [2-507](#)

reconfirming dynamic VLAN assignments [2-505](#)

vmmps reconfirm (global configuration) command [2-504](#)

vmmps reconfirm (privileged EXEC) command [2-505](#)

vmmps retry command [2-506](#)

vmmps server command [2-507](#)

voice VLANs

enabling [2-457](#)

VoIP

configuring auto-QoS [2-10](#)

VQP

per-server retry count [2-506](#)

reconfirming dynamic VLAN assignments [2-505](#)

VTP

configuring the administrative domain name [2-511](#)

configuring the device in VTP client mode [2-510](#)

configuring the device in VTP server mode [2-514](#)

configuring the device in VTP transparent mode [2-515](#)

configuring tunnel encapsulation rate [2-160](#)

creating a VTP domain password [2-512](#)

displaying domain information [2-409](#)

displaying statistics information [2-409](#)

enabling protocol tunneling for [2-157](#)

enabling pruning in the VLAN database [2-513](#)

enabling VTP version 2 mode [2-516](#)

modifying the VTP configuration storage file
name [2-509](#)

set drop threshold for [2-159](#)

VTP protocol code

activating debug messages [2-74](#)

deactivating debug messages [2-74](#)



Acronyms

A

ACE	access control entry
ACL	access control list
AFI	authority and format identifier
Agport	aggregation port
AMP	Active Monitor Present
APaRT	Automated Packet Recognition and Translation
ARP	Address Resolution Protocol

B

BGP	Border Gateway Protocol
BPDU	bridge protocol data unit
BRF	bridge relay function
BSC	Bisync
BSTUN	Block Serial Tunnel
BUS	broadcast and unknown server
BVI	bridge-group virtual interface

C

CAM	content-addressable memory
CAR	committed access rate
CCA	circuit card assembly
CDP	Cisco Discovery Protocol
CEF	Cisco Express Forwarding
CHAP	Challenge Handshake Authentication Protocol
CIR	committed information rate
CLI	command-line interface
CLNS	Connection-Less Network Service
CMNS	Connection-Mode Network Service
COPS	Common Open Policy Server
COPS-DS	Common Open Policy Server Differentiated Services
CoS	class of service
CPLD	Complex Programmable Logic Device
CRC	cyclic redundancy check
CRF	concentrator relay function
CST	Common Spanning Tree

D

DAI	Dynamic ARP Inspection
DBL	Dynamic Buffer Limiting
DCC	Data Country Code
dCEF	distributed Cisco Express Forwarding
DDR	dial-on-demand routing
DE	discard eligibility

DEC	Digital Equipment Corporation
DFI	Domain-Specific Part Format Identifier
DFP	Dynamic Feedback Protocol
DISL	Dynamic Inter-Switch Link
DLC	Data Link Control
DLSw	Data Link Switching
DMP	data movement processor
DNS	Domain Name System
DoD	Department of Defense
DOS	denial of service
DRAM	dynamic RAM
DRiP	Dual Ring Protocol
DSAP	destination service access point
DSCP	differentiated services code point
DSPU	downstream SNA Physical Units
DTP	Dynamic Trunking Protocol
DTR	data terminal ready
DVMRP	Distance Vector Multicast Routing Protocol
DXI	data exchange interface

E

EAP	Extensible Authentication Protocol
EARL	Enhanced Address Recognition Logic
EEPROM	electrically erasable programmable read-only memory
EHSA	enhanced high system availability

EIA	Electronic Industries Association
ELAN	Emulated Local Area Network
EOBC	Ethernet out-of-band channel
ESI	end-system identifier

F

FECN	forward explicit congestion notification
FM	feature manager
FRU	field replaceable unit
FSM	feasible successor metrics

G

GARP	General Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
GVRP	GARP VLAN Registration Protocol

I

ICC	Inter-card Communication
ICD	International Code Designator
ICMP	Internet Control Message Protocol
IDB	interface descriptor block
IDP	initial domain part or Internet Datagram Protocol
IDPROM	ID Programmable Read-Only Memory
IFS	IOS File System
IGMP	Internet Group Management Protocol
IGRP	Interior Gateway Routing Protocol

ILMI	Integrated Local Management Interface
IP	Internet Protocol
IPC	interprocessor communication
IPX	Internetwork Packet Exchange
IS-IS	Intermediate System-to-Intermediate System Intradomain Routing Protocol
ISL	Inter-Switch Link
ISO	International Organization of Standardization
ISR	Integrated SONET router

L

L2	Layer 2
L3	Layer 3
L4	Layer 4
LAN	local area network
LANE	LAN Emulation
LAPB	Link Access Procedure, Balanced
LDA	Local Director Acceleration
LCP	Link Control Protocol
LEC	LAN Emulation Client
LECS	LAN Emulation Configuration Server
LEM	link error monitor
LER	link error rate
LES	LAN Emulation Server
LLC	Logical Link Control
LTL	Local Target Logic

M

MAC	Media Access Control
MD5	Message Digest 5
MET	Multicast Expansion Table
MFIB	Multicast Forwarding Information Base
MIB	Management Information Base
MII	media-independent interface
MLS	Multilayer Switching
MLSE	maintenance loop signaling entity
MOP	Maintenance Operation Protocol
MOTD	message-of-the-day
MRM	multicast routing monitor
MRQ	Multicast Replication Queue
MSDP	Multicast Source Discovery Protocol
MST	Multiple Spanning Tree
MTU	maximum transmission unit
MVAP	multiple VLAN access port

N

NBP	Name Binding Protocol
NCIA	Native Client Interface Architecture
NDE	NetFlow Data Export
NET	network entity title
NetBIOS	Network Basic Input/Output System
NFFC	NetFlow Feature Card
NMP	Network Management Processor

NSAP	network service access point
NTP	Network Time Protocol
NVRAM	nonvolatile RAM

O

OAM	Operation, Administration, and Maintenance
OSI	Open System Interconnection
OSPF	open shortest path first

P

PAE	port access entity
PAgP	Port Aggregation Protocol
PBD	packet buffer daughterboard
PC	Personal Computer (formerly PCMCIA)
PCM	pulse code modulation
PCR	peak cell rate
PDP	policy decision point
PDU	protocol data unit
PEM	Power Entry Module
PEP	policy enforcement point
PGM	Pragmatic General Multicast
PHY	physical sublayer
PIB	policy information base
PIM	Protocol Independent Multicast
PM	Port manager
PPP	Point-to-Point Protocol

PRID	Policy Rule Identifiers
PVLAN	Private VLAN
PVST+	Per VLAN Spanning Tree+

Q

QM	QoS manager
QoS	quality of service

R

RACL	router interface access control list
RADIUS	Remote Access Dial-In User Service
RAM	random-access memory
RCP	Remote Copy Protocol
RGMP	Router Group Management Protocol
RIF	Routing Information Field
RMON	remote network monitor
ROM	read-only memory
RP	route processor or rendezvous point
RPC	remote procedure call
RPF	reverse path forwarding
RPR	Router Processor Redundancy
RSPAN	remote SPAN
RST	reset
RSVP	ReSerVation Protocol
Rx	Receive

S

SAID	Security Association Identifier
SAP	service access point
SCM	service connection manager
SCP	Switch-Module Configuration Protocol
SDLC	Synchronous Data Link Control
SGBP	Stack Group Bidding Protocol
SIMM	single in-line memory module
SLB	server load balancing
SLCP	Supervisor Line-Card Processor
SLIP	Serial Line Internet Protocol
SMDS	Software Management and Delivery Systems
SMF	software MAC filter
SMP	Standby Monitor Present
SMRP	Simple Multicast Routing Protocol
SMT	Station Management
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyzer
SRB	source-route bridging
SRT	source-route transparent bridging
SSTP	Cisco Shared Spanning Tree
STP	Spanning Tree Protocol
SVC	switched virtual circuit
SVI	switched virtual interface

T

TACACS+	Terminal Access Controller Access Control System Plus
TARP	Target Identifier Address Resolution Protocol
TCAM	Ternary Content Addressable Memory
TCL	table contention level
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
TIA	Telecommunications Industry Association
TLV	type-length-value
TopN	Utility that allows the user to analyze port traffic by reports
TOS	type of service
TrBRF	Token Ring Bridge Relay Function
TrCRF	Token Ring Concentrator Relay Function
TTL	Time To Live
TVX	valid transmission
Tx	Transmit

U

UDLD	UniDirectional Link Detection Protocol
UDP	User Datagram Protocol
UNI	User-Network Interface
UTC	Coordinated Universal Time

V

VACL	VLAN access control list
------	--------------------------

VCC	virtual channel circuit
VCD	virtual circuit descriptor
VCI	virtual circuit identifier
VCR	Virtual Configuration Register
VINES	Virtual Network System
VLAN	virtual LAN
VMPS	VLAN Membership Policy Server
VTP	VLAN Trunking Protocol
VVID	voice VLAN ID

W

WFQ	weighted fair queueing
WRED	weighted random early detection
WRR	weighted round-robin

X

XNS	Xerox Network System
-----	----------------------



Acknowledgments for Open-Source Software

The Catalyst operating system 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.

