



Catalyst 4500 Series Switch Cisco IOS Command Reference

Release 12.2(46)SG

Americas Headquarters

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

Text Part Number: OL-16005-01

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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0805R)

Catalyst 4500 Series Switch Cisco IOS Command Reference Copyright © 2008 Cisco Systems, Inc. All rights reserved



CONTENTS

Preface xvii

Audience xvii Organization xvii Related Documentation xvii Conventions xviii Notices xix Obtaining Documentation, Obtaining Support, and Security Guidelines xxi

Command-Line Interface 1-1

Getting Help 1-1 How to Find Command Options 1-2 Understanding Command Modes 1-5 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

Cisco IOS Commands for the Catalyst 4500 Series Switches 2-1

#macro keywords 2-2 aaa accounting dot1x default start-stop group radius 2-4 aaa accounting system default start-stop group radius 2-5 access-group mode **2-6** access-list hardware capture mode 2-8 access-list hardware entries 2-10 access-list hardware region 2-12 action 2-13 apply 2-14 arp access-list 2-16 attach module 2-17 auto gos voip 2-18 auto-sync 2-21 bandwidth 2-22

channel-group 2-25 channel-protocol 2-27 class 2-29 class-map 2-32 clear counters 2-34 clear hw-module slot password 2-36 clear interface gigabitethernet 2-37 clear interface vlan 2-38 clear ip access-template 2-39 clear ip arp inspection log 2-40 clear ip arp inspection statistics 2-41 clear ip dhcp snooping binding 2-42 clear ip dhcp snooping database 2-44 clear ip dhcp snooping database statistics 2-45 clear ip igmp group 2-46 clear ip igmp snooping membership 2-48 clear ip mfib counters 2-49 clear ip mfib fastdrop 2-50 clear lacp counters 2-51 clear mac-address-table 2-52 clear mac-address-table dynamic 2-54 clear pagp 2-55 clear port-security 2-56 clear gos 2-58 clear vlan counters 2-60 clear vmps statistics 2-61 control-plane 2-62 counter 2-64 dbl 2-65 debug adjacency 2-67 debug backup 2-68 debug condition interface 2-69 debug condition standby 2-70 debug condition vlan 2-72 debug dot1x 2-74

debug etherchnl 2-75 debug interface 2-77 debug ipc 2-78 debug ip dhcp snooping event 2-79 debug ip dhcp snooping packet 2-80 debug ip verify source packet 2-81 debug lacp 2-82 debug monitor 2-83 debug nvram 2-84 2-85 debug pagp debug platform packet protocol lacp 2-86 debug platform packet protocol pagp 2-87 debug pm 2-88 debug port-security 2-89 debug redundancy 2-90 debug spanning-tree 2-91 debug spanning-tree backbonefast 2-93 debug spanning-tree switch 2-94 debug spanning-tree uplinkfast 2-96 debug sw-vlan 2-97 debug sw-vlan ifs 2-98 debug sw-vlan notification 2-100 debug sw-vlan vtp 2-101 debug udld 2-102 debug vqpc 2-104 define interface-range 2-105 deny 2-106 diagnostic monitor action 2-108 diagnostic start 2-109 dot1x auth-fail max-attempts 2-110 dot1x auth-fail vlan 2-111 dot1x control-direction **2-112** dot1x critical 2-113 dot1x critical eapol 2-114

dot1x critical recovery delay 2-115 dot1x critical vlan 2-116 dot1x guest-vlan 2-117 dot1x guest-vlan supplicant 2-118 dot1x host-mode 2-119 dot1x initialize 2-121 dot1x mac-auth-bypass 2-122 dot1x max-reauth-req 2-123 dot1x max-req 2-124 dot1x port-control 2-126 dot1x re-authenticate 2-128 dot1x re-authentication 2-129 dot1x system-auth-control 2-130 dot1x timeout 2-131 duplex 2-133 erase 2-135 errdisable detect 2-138 errdisable recovery 2-140 flowcontrol 2-143 hardware statistics 2-146 hw-module port-group 2-147 hw-module power 2-148 hw-module uplink mode shared-backplane 2-149 hw-module uplink select 2-151 instance 2-153 interface 2-155 interface port-channel 2-157 interface range 2-158 interface vlan 2-160 ip arp inspection filter vlan 2-161 ip arp inspection limit (interface) 2-163 ip arp inspection log-buffer 2-165 ip arp inspection trust 2-167 ip arp inspection validate 2-168 ip arp inspection vlan 2-170

I

ip arp inspection vlan logging 2-172 ip cef load-sharing algorithm 2-174 ip device tracking maximum 2-176 ip dhcp snooping 2-177 ip dhcp snooping binding 2-178 ip dhcp snooping database 2-180 ip dhcp snooping information option 2-182 ip dhcp snooping information option allow-untrusted 2-184 ip dhcp snooping limit rate 2-185 ip dhcp snooping trust 2-186 ip dhcp snooping vlan 2-187 ip dhcp snooping vlan number information option format-type 2-189 ip igmp filter **2-191** ip igmp max-groups 2-192 ip igmp profile 2-193 ip igmp query-interval 2-194 ip igmp snooping 2-196 ip igmp snooping report-suppression 2-198 ip igmp snooping vlan 2-200 ip igmp snooping vlan explicit-tracking 2-201 ip igmp snooping vlan immediate-leave 2-203 ip igmp snooping vlan mrouter 2-205 ip igmp snooping vlan static 2-207 ip local-proxy-arp 2-209 ip mfib fastdrop 2-210 ip route-cache flow 2-211 ip source binding 2-213 ip sticky-arp 2-214 ip verify header vlan all 2-216 ip verify source 2-217 ip verify unicast source reachable-via 2-219 ipv6 mld snooping 2-221 ipv6 mld snooping last-listener-query-count 2-223

ipv6 mld snooping last-listener-query-interval 2-225 ipv6 mld snooping listener-message-suppression 2-227 ipv6 mld snooping robustness-variable 2-228 ipv6 mld snooping tcn 2-230 ipv6 mld snooping vlan 2-231 issu abortversion 2-233 issu acceptversion 2-235 issu commitversion 2-237 issu loadversion 2-239 issu runversion 2-241 issu set rollback-timer 2-242 I2protocol-tunnel 2-243 l2protocol-tunnel cos 2-245 I2protocol-tunnel drop-threshold 2-246 I2protocol-tunnel shutdown-threshold 2-248 lacp port-priority 2-250 lacp system-priority 2-251 logging event link-status global (global configuration) 2-252 logging event link-status (interface configuration) 2-253 logging event trunk-status global (global configuration) 2-255 logging event trunk-status (interface configuration) 2-256 mac access-list extended 2-258 mac-address-table aging-time 2-261 mac-address-table dynamic group protocols 2-262 mac-address-table notification 2-265 mac-address-table static 2-267 2-268 macro apply cisco-desktop macro apply cisco-phone 2-270 macro apply cisco-router 2-272 macro apply cisco-switch 2-274 macro global apply cisco-global 2-276 macro global apply system-cpp 2-277 macro global description 2-278 main-cpu 2-279 match 2-281

match (class-map configuration) 2-283 match flow ip 2-286 mdix auto 2-290 media-type 2-292 mode 2-293 monitor session 2-295 mtu 2-301 2-302 name pagp learn-method 2-303 pagp port-priority 2-304 passive-interface 2-305 permit 2-308 police 2-310 police (percent) 2-315 police rate 2-317 police (two rates) 2-319 policy-map 2-323 port-channel load-balance 2-325 power dc input 2-327 power inline 2-328 power inline consumption 2-330 power redundancy-mode 2-331 port-security mac-address 2-333 port-security mac-address sticky 2-334 port-security maximum 2-335 priority 2-337 private-vlan 2-339 private-vlan mapping 2-343 private-vlan synchronize 2-346 qos (global configuration mode) 2-347 gos (interface configuration mode) 2-348 qos account layer2 encapsulation 2-349 qos aggregate-policer 2-351 qos control-packets 2-354 2-356 qos cos

qos dbl 2-357 qos dscp 2-360 qos map cos 2-361 qos map dscp 2-363 qos map dscp policed 2-365 qos rewrite ip dscp 2-367 qos trust 2-368 qos vlan-based 2-370 queue-limit 2-372 redundancy 2-374 redundancy config-sync mismatched-commands 2-376 redundancy force-switchover 2-378 redundancy reload 2-379 remote login module 2-380 remote-span 2-381 renew ip dhcp snooping database 2-382 reset 2-383 revision 2-384 service-policy (interface configuration) 2-385 service-policy (policy-map class) 2-388 service-policy input (control-plane) 2-390 session module 2-392 set 2-394 set cos 2-396 set dscp 2-399 set precedence 2-402 set qos-group 2-405 shape (class-based queueing) 2-407 shape (interface configuration) 2-409 show access-group mode interface 2-411 show adjacency 2-412 show arp access-list 2-414 show auto install status 2-415 show auto qos 2-416

show bootflash: 2-417 show bootvar 2-419 show cable-diagnostics tdr 2-420 show cdp neighbors 2-422 show class-map 2-425 show diagnostic content 2-427 show diagnostic result module 2-429 show diagnostic result module test 2-433 show diagnostic result module test 2 2-435 show diagnostic result module test 3 2-437 show dot1x 2-439 show environment 2-443 show errdisable detect 2-446 show errdisable recovery 2-447 show etherchannel 2-449 show flowcontrol 2-453 show hw-module port-group 2-455 show hw-module uplink 2-456 show idprom 2-457 show interfaces 2-463 show interfaces capabilities 2-466 show interfaces counters 2-470 show interfaces description 2-472 show interfaces link 2-473 show interfaces mtu 2-474 show interfaces private-vlan mapping 2-475 show interfaces status 2-476 show interfaces switchport 2-478 show interfaces transceiver 2-480 show interfaces trunk 2-485 show ip arp inspection 2-487 show ip arp inspection log 2-490 show ip cef vlan 2-492 show ip dhcp snooping 2-493

show ip dhcp snooping binding 2-495 show ip dhcp snooping database 2-498 show ip igmp interface 2-500 show ip igmp profile 2-502 show ip igmp snooping 2-503 show ip igmp snooping membership 2-507 show ip igmp snooping mrouter 2-509 show ip igmp snooping vlan 2-510 show ip interface 2-512 show ip mfib 2-515 show ip mfib fastdrop 2-517 show ip mroute 2-518 show ip source binding 2-523 show ip verify source 2-525 show ipc 2-528 show ipv6 mld snooping 2-530 show ipv6 mld snooping mrouter 2-532 show ipv6 mld snooping querier 2-533 show issu capability 2-535 show issu clients 2-537 show issu comp-matrix 2-539 show issu endpoints 2-544 show issu entities 2-545 show issu fsm 2-546 show issu message 2-547 show issu negotiated 2-549 show issu rollback-timer 2-550 show issu sessions 2-551 show issu state 2-552 show I2protocol-tunnel 2-554 show lacp 2-557 show mac access-group interface 2-560 show mac-address-table address 2-561

show mac-address-table aging-time 2-563 show mac-address-table count **2-565** show mac-address-table dynamic 2-567 show mac-address-table interface 2-569 show mac-address-table multicast 2-571 show mac-address-table notification 2-573 show mac-address-table protocol 2-575 show mac-address-table static 2-577 show mac-address-table vlan 2-580 show module 2-582 show monitor 2-584 show pagp 2-586 show policy-map 2-588 show policy-map control-plane 2-589 show policy-map interface 2-592 show policy-map interface vlan 2-595 show port-security 2-597 show power 2-604 show qos 2-611 show qos aggregate policer 2-612 show gos dbl 2-613 show qos interface 2-614 show gos maps 2-616 show redundancy 2-618 show redundancy config-sync 2-622 show running-config 2-625 show slavebootflash: 2-627 show slaveslot0: 2-629 show slot0: 2-631 show spanning-tree 2-633 show spanning-tree mst 2-638 show storm-control 2-641 show system mtu 2-643 show tech-support 2-644 show udld 2-646

show vlan 2-648 show vlan access-map 2-652 show vlan counters 2-653 show vlan dot1q tag native 2-654 show vlan internal usage 2-655 show vlan mtu 2-656 show vlan private-vlan 2-657 show vlan remote-span 2-659 show vmps 2-660 show vtp **2-662** snmp ifindex clear 2-665 snmp ifindex persist 2-667 snmp-server enable traps 2-669 snmp-server ifindex persist 2-671 snmp-server ifindex persist compress 2-672 snmp trap mac-notification change 2-673 spanning-tree backbonefast 2-674 spanning-tree bpdufilter 2-675 spanning-tree bpduguard 2-677 spanning-tree cost 2-678 spanning-tree etherchannel guard misconfig 2-679 spanning-tree extend system-id 2-680 spanning-tree guard 2-681 spanning-tree link-type 2-682 spanning-tree loopguard default 2-683 spanning-tree mode 2-684 spanning-tree mst 2-685 spanning-tree mst configuration 2-687 spanning-tree mst forward-time 2-689 spanning-tree mst hello-time 2-690 spanning-tree mst max-age 2-691 spanning-tree mst max-hops 2-692 spanning-tree mst root 2-693 spanning-tree pathcost method 2-695

spanning-tree portfast (interface configuration mode) 2-696 spanning-tree portfast bpdufilter default 2-698 spanning-tree portfast bpduguard default 2-700 spanning-tree portfast default 2-701 spanning-tree port-priority 2-702 spanning-tree uplinkfast 2-703 spanning-tree vlan 2-705 speed 2-707 storm-control 2-710 storm-control broadcast include multicast 2-712 switchport 2-713 switchport access vlan 2-715 switchport autostate exclude 2-717 switchport block 2-719 switchport mode 2-720 switchport port-security 2-725 switchport private-vlan association trunk 2-730 switchport private-vlan host-association 2-732 switchport private-vlan mapping 2-734 switchport private-vlan trunk allowed vlan 2-737 switchport private-vlan trunk native vlan tag 2-740 switchport trunk 2-741 system mtu 2-745 test cable-diagnostics tdr 2-747 traceroute mac 2-749 traceroute mac ip 2-752 trust 2-755 tx-queue 2-757 udld (global configuration mode) 2-759 udld (interface configuration mode) 2-761 udld reset 2-763 unidirectional 2-764 username 2-765 verify 2-767

vlan (VLAN Database mode) 2-769 vlan access-map 2-772 vlan configuration 2-774 vlan database 2-776 vlan dot1q tag native 2-778 vlan filter 2-780 vlan internal allocation policy 2-781 vmps reconfirm (global configuration) 2-782 vmps reconfirm (privileged EXEC) 2-783 vmps retry 2-784 vmps server 2-785 vtp (global configuration mode) 2-787 vtp client 2-788 vtp domain 2-789 vtp password 2-790 vtp pruning 2-791 vtp server 2-792 vtp transparent 2-793 vtp v2-mode 2-794

APPENDIX A

Abbreviations A-1

INDEX

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 Catalyst 4500 series switches.

Organization

This publication is organized as follows:

Chapter	Title	Description
Chapter 1	Command-Line Interface	Describes the Catalyst 4500 series switch CLI.
Chapter 2	Cisco IOS Commands for the Catalyst 4500 Series Switches	Lists all Catalyst 4500 series Cisco IOS commands alphabetically and provides detailed information on each command.
Appendix A	Abbreviations	Defines the acronyms used in this publication.

Related Documentation

The Catalyst 4500 series Cisco IOS documentation set includes these publications:

- Catalyst 4500 Series Switch Installation Guide
- Catalyst 4500 Series Switch Supervisor Engine III Installation Note
- Catalyst 4500 Series Switch Supervisor Engine IV Installation Note
- Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide
- Catalyst 4500 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 12.2 Configuration Guides
- Cisco IOS Release 12.2 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.
italic font	<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.
$[\mathbf{x} \mid y]$	Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.
$\{\mathbf{x} \mid y\}$	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</i> font	Arguments for which you supply values are in <i>italic screen</i> font.
^	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.
[]	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:



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

Cautions use this convention:



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

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
- 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
- **3.** All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".
- 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
- 5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

L

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- **1.** Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
- 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- **3.** All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO

EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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

Γ



CHAPTER

Command-Line Interface

This chapter provides information for understanding and using the Cisco IOS command-line interface (CLI) on the Catalyst 4500 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 1-5
- 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 Catalyst 4500 series switch Cisco IOS configuration, refer to the *Catalyst 4500* 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.

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

Table 1-1 Getting Help

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 Catalyst 4500 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**?

Table 1-2 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

Command	Purpose
Switch> enable Password: <password> Switch#</password>	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 global configuration mode.
Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#	You are in global configuration mode when the prompt changes to Switch(config)#.
<pre>Switch(config)# interface gigabitethernet ? <1-9> GigabitEthernet interface number Switch(config)# interface gigabitethernet 1/1 Switch(config-if)#</pre>	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)#.

Table 1-2How to Find Command Options

Table 1-2	How to Find Command Options (continued)
-----------	---

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

Table 1-2	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>	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.
	Because a <cr>> is not displayed, it indicates that you must enter more information to complete the command.</cr>
<pre>Switch(config-if)# channel-group 1 ? mode Etherchannel Mode of the interface Switch(config-if)#</pre>	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.
	Because a <cr> is not displayed, it indicates that you must enter more information to complete the command.</cr>
<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>	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.
	Because a <cr>> is not displayed, it indicates that you must enter more information to complete the command.</cr>
<pre>Switch(config-if)# channel-group 1 mode auto ?</pre>	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.
	Because a <cr>> 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.</cr>
<pre>Switch(config-if)# channel-group 1 mode auto Switch(config-if)#</pre>	In this example, press Return to complete the command.

Understanding Command Modes

The Cisco IOS user interface on the Catalyst 4500 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 Catalyst 4500 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 Catalyst 4500 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 Catalyst 4500 series switch cannot boot properly. If your Catalyst 4500 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.

Command Mode	Access Method	Prompt	Exit Method
User EXEC mode	Log in.	Switch>	Use the logout command.
Privileged EXEC mode	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 mode	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 mode	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.

Table 1-3 Summary of Main Command Modes

Γ

Command Mode	Access Method	Prompt	Exit Method
Subinterface configuration	From interface configuration mode, specify a subinterface	Switch(config-subif)#	To exit to global configuration mode, enter the exit command.
	with an interface 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 <i>filename</i> command).

Table 1-3 Summary of Main Command Modes (continued)

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 ip routing** 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 though 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 \sim) 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.

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.

Table 1-4 Characters with Special Meaning

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 ($^{\wedge}$) 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.

Γ

Alternation

Alternation allows you to specify alternative patterns to match against a string. You separate the alternative patterns with a vertical bar (I). 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 Table 1-6.

Table 1-6 Special Characters Used for Anchoring

Character	Description	
٨	Matches the beginning of the string.	
\$	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 page 1-9, 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.



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 Cisco IOS commands for the Catalyst 4500 series switches. For information about Cisco IOS commands that are not included in this publication, refer to Cisco IOS Release 12.2 configuration guides and command references 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 the 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. Global configuration mode 		
Command Modes			
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 the #macro keywords command, 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 gi1/1 Switch(config-if)# macro apply test ? WORD Keyword to replace with a value e.g \$VLAN, \$MAX << It is shown as help <cr></cr>		
Related Commands	Command	Description	
------------------	---------------------------	--	
	macro apply cisco-desktop	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop.	
	macro apply cisco-phone	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop and a Cisco IP phone.	
	macro apply cisco-router	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a router.	
	macro apply cisco-switch	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to another switch.	

aaa accounting dot1x default start-stop group radius

To enable accounting for 802.1X authentication sessions, use the **aaa accounting dot1x default start-stop group radius** command. To disable accounting, use the **no** form of this command.

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 mode

 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

This example shows how to configure 802.1X accounting:

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

```
<u>Note</u>
```

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

Related Commands	Command	Description
aaa accounting system o		Receives the session termination messages after the switch
	start-stop group radius	reboots.

Γ

aaa accounting system default start-stop group radius

To receive the session termination messages after the switch reboots, use the **aaa accounting system** default start-stop group radius command. To disable accounting, use the no form of this command. 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 Modification **Command History** Release 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** This 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	Command	Description	
	e e e e e e e e e e e e e e e e e e e	Enables accounting for 802.1X authentication sessions.	
	start-stop group radius		

access-group mode

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

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 vlanSpecifies that the VLAN-based ACL mode take precedence. If no VLAN-ba ACL features are configured on the port's VLAN, the PACL features on the are applied.	
	merge	Merges applicable ACL features before they are programmed into the hardware.
Defaults	PACL override n	node
Command Modes	Interface configu	iration mode
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 Layer 2 interface can have one IP ACL applied in either direction (one inbound and one outbound).	
Examples	This example sho	ows how to make the PACL mode on the switch take effect:
	(config-if)# ac	ccess-group mode prefer port
	This example sho	ows how to merge applicable ACL features:
	(config-if)# access-group mode merge	

Related Commands	Command	Description
	show access-group modeDisplays the ACL configuration on a Layer 2 interfaceinterface	
	show ip interface (refer to Cisco IOS documentation)	Displays the IP interface configuration.
	show mac access-groupDisplays the ACL configuration on a Layer 2 interface.interface	

access-list hardware capture mode

To select the mode of capturing control packets, use the access-list hardware capture mode command.

access-list hardware capture mode {global | vlan}

```
Syntax Description
                     global
                                            Specifies the capture of control packets globally on all VLANs.
                     vlan
                                            Specifies the capture of control packets on a specific VLAN.
Defaults
                     The control packets are globally captured.
Command Modes
                     Global configuration mode
                                       Modification
Command History
                     Release
                     12.2(40)SG
                                       Support for this command was introduced on the Catalyst 4500 series switch.
Usage Guidelines
                     This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.
                     Before configuring the capture mode, it is best to examine and modify your configuration to globally
                     disable features such as DHCP snooping or IGMP snooping, and instead enable them on specific
                     VLANs.
                     When changing to path managed mode, be aware that control traffic may be bridged in hardware or
                     dropped initially until the per-vlan CAM entries are programmed in hardware.
                     You must ensure that any access control configuration on a member port or VLAN does not deny or drop
                     the control packets from being forwarded to the CPU for the features which are enabled on the VLAN.
                     If control packets are not permitted then the specific feature does not function.
Examples
                     This example shows how to configure the switch to capture control packets on VLANs that are
                     configured to enable capturing control packets.
                     Switch# configure terminal
                     Enter configuration commands, one per line. End with CNTL/Z.
                     Switch(config)# access-list hardware capture mode vlan
                     Switch(config)# end
                     Switch#
                     This example shows how to configure the switch to capture control packets globally across all VLANs
                     (using a static ACL).
                     Switch# configure terminal
                     Enter configuration commands, one per line. End with CNTL/Z.
                     Switch(config)# access-list hardware capture mode global
                     Switch(config)# end
                     Switch#
```

This example shows another way to configure the switch to capture control packets globally across all VLANs.

Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# no access-list hardware capture mode vlan Switch(config)# end Switch#

access-list hardware entries

To designate how ACLs are programmed into the switch hardware, use the **access-list hardware entries** command.

access-list hardware entries {packed | scattered}

Syntax Description	packed	Directs the software to use the first entry with a matching mask when selecting an entry from the ACL TCAM for programming the ACEs in an ACL.	
	scattered	Directs the software to use the first entry with a free mask when selecting an entry from the ACL TCAM for programming the ACEs in an ACL.	
Defaults	The ACLs are pro	ogrammed as packed.	
Command Modes	Global configura	tion mode	
Command History	Release	Modification	
	12.2(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.	
	Two types of hardware resources are used when ACLs are programmed: entries and masks. If one of these resources is consumed, no additional ACLs can be programmed into the hardware. If the masks are consumed, but the entries are available, change the programming algorithm from packed to scattered to make the masks available. This action allows additional ACLs to be programmed into the hardware. The goal is to use TCAM resources more efficiently; that is, to minimize the number of masks per ACL entries. To compare TCAM utilization when using the scattered or packed algorithms, use the show platform hardware acl statistics utilization brief command. To change the algorithm from packed to scattered , use the access-list hardware entries command.		
Examples	_	ows how to program ACLs into the hardware as packed. After they are programmed, you cent of the masks to program only 49 percent of the ACL entries.	
	Switch# configura Enter configura Switch(config)# Switch(config)# Switch# 01:15:34: %SYS- Switch# Switch# show pl	are terminal ation commands, one per line. End with CNTL/Z. # access-list hardware entries packed	
	Inp Inp	put Acl(PortAndVlan) 2016 / 4096 (49) 460 / 512 (89) put Acl(PortOrVlan) 6 / 4096 (0) 4 / 512 (0) put Qos(PortAndVlan) 0 / 4096 (0) 0 / 512 (0) put Qos(PortOrVlan) 0 / 4096 (0) 0 / 512 (0)	

Output Acl(PortAndVlan)	0 / 4096 (0)	0 /	512 (0)
Output Acl(PortOrVlan)	0 / 4096 (0)	0 /	512 (0)
Output Qos(PortAndVlan)	0 / 4096 (0)	0 /	512 (0)
Output Qos(PortOrVlan)	0 / 4096 (0)	0 /	512 (0)
L4Ops: used 2 out of 64				

Switch#

This example shows how to reserve space (scatter) between ACL entries in the hardware. The number of masks required to program 49 percent of the entries has decreased to 49 percent.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) # access-list hardware entries scattered
Switch(config)# end
Switch#
01:39:37: %SYS-5-CONFIG_I: Configured from console by console
Switch#
Switch# show platform hardware acl statistics utilization brief
Entries/Total(%) Masks/Total(%)
                                    _____
           Input Acl(PortAndVlan) 2016 / 4096 ( 49) 252 / 512 ( 49)
                                   6 / 4096 ( 0)
                                                   5 / 512 ( 0)
           Input Acl(PortOrVlan)
           Input Qos(PortAndVlan)
                                    0 / 4096 ( 0)
                                                     0 / 512 ( 0)
           Input Qos(PortOrVlan)
                                   0 / 4096 ( 0)
                                                     0 / 512 ( 0)
           Output Acl(PortAndVlan)
                                   0 / 4096 ( 0)
                                                     0 / 512 ( 0)
           Output Acl(PortOrVlan)
                                    0 / 4096 ( 0)
                                                     0 / 512 (
                                                                 0)
           Output Qos(PortAndVlan)
                                    0 / 4096 ( 0)
                                                      0 / 512 (
                                                                 0)
           Output Qos(PortOrVlan)
                                    0 / 4096 ( 0)
                                                      0 / 512 (
                                                                 0)
          L4Ops: used 2 out of 64
```

Switch#

access-list hardware region

To modify the balance between TCAM regions in hardware, use the **access-list hardware region** command.

access-list hardware region {feature | qos} {input | output} balance {bal-num}

Syntax Description	feature	Specifies adjustment of region balance for ACLs.	
	qos	Specifies adjustment of region balance for QoS.	
	input Specifies adjustment of region balance for input ACL and QoS.		
	output	Specifies adjustment of region balance for output ACL and QoS.	
	balance bal-num	Specifies relative sizes of the PandV and PorV regions in the TCAM; valid values are between 1 and 99.	
Defaults	The default region balance for each TCAM is 50.		
Command Modes	Global configurat	ion mode	
Command History	Release	Modification	
	12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switch.	
Usage Guidelines		I region containing entries which mask in both the port and VLAN tag portions of the	
	flow label.		
	PorV is a TCAM region containing entries which mask in either the port or VLAN tag porti flow label, but not both.		
	A balance of 1 allocates the minimum number of PandV region entries and the maximum PorV region entries. A balance of 99 allocates the maximum number of PandV region entries minimum number of PorV region entries. A balance of 50 allocates equal numbers of Pan region entries in the specified TCAM.		
	Balances for the f	our TCAMs can be modified independently.	
Examples	This example sho	ws how to enable the MAC notification trap when a MAC address is added to a port:	
	Switch# configure terminal Switch(config)# access-list hardware region feature input balance 75 Switch(config)#		

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}

		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).			
		f an ACL for a packet type is configured and the ACL is empty or undefined, the configured action will e applied to the packet type.		
Examples	This example s	hows 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 Switch(config	-access-map)# action forward -access-map)#		
Syntax Description	Command	Description		
-	match	Specifies a match clause by selecting one or more ACLs for a VLAN access-map sequence.		
	show vlan acc	ess-map Displays the contents of a VLAN access map.		
	vlan access-map Enters VLAN access-map command mode to creat 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 keyword	s.
---	----

- **Defaults** This command has no default settings.
- Command Modes VLAN configuration mode

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 that 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 the 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	Command	Description
	exit (refer to Cisco IOS documentation)	Closes an active terminal session by logging off the switch.
	reset	Leaves the proposed new VLAN database but remains in VLAN configuration mode and resets the proposed new database to be identical to the VLAN database currently implemented.
	show vlan	Displays VLAN information.

Command	Description
shutdown vlan (refer to Cisco IOS documentation)	Shutsdown VLAN switching.
vtp (global configuration mode)	Modifies the name of a VTP configuration storage file.

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	name Speci	fies 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	-	s how to define an ARP access list named static-hosts:
Related Commands	Command	Description
	deny	Denies an ARP packet based on matches against the DHCP bindings.
	ip arp inspection f	filter vlanPermits ARPs from hosts that are configured for static IP when DAI is enabled and to define an ARP access list and applies it to a VLAN.
	permit	Permits an ARP packet based on matches against the DHCP bindings.

attach module

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

attach module mod

Syntax Description	<i>mod</i> Target mode	ule for the command.	
Defaults	This command has no default settings.		
Command Modes	Privileged		
Command History	Release	Modification	
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.	
Usage Guidelines	The valid values for <i>mod</i> chassis, valid values for 73 to 7. When you execute the at	nly to the Access Gateway Module on Catalyst 4500 series switches. I depend on the chassis that are used. For example, if you have a Catalyst 4506 the module are from 2 to 6. If you have a 4507R chassis, valid values are from Etach module <i>mod</i> command, the prompt changes to Gateway#. al in the resulting action to the session module <i>mod</i> and the remote login	
Examples	Switch# attach module Attaching console to m		
Related Commands	Command	Description	
	remote login module	Remotely connects to a specific module.	
	session module	Logs in to the standby supervisor engine using a virtual console.	

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. To change the auto-QoS configuration settings to the standard QoS defaults, use the **no** form of this command.

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	trustConnects 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 dis	abled on all interfaces.				
Command Modes	Interface config	uration mode				
Command History	Release	Modification				
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.				
Usage Guidelines		nd to configure the QoS that is appropriate for VoIP traffic within the QoS domain. The				
Jsage Guidelines	QoS domain inc incoming traffic Use the cisco-pl phones. The swi	ludes the switch, the interior of the network, and the edge devices that can classify				
sage Guidelines	QoS domain inc incoming traffic Use the cisco-pl phones. The swi labels in packets Use the trust ke	ludes the switch, the interior of the network, and the edge devices that can classify for QoS. none keyword on the ports at the edge of the network that are connected to Cisco IP tch detects the telephone through the Cisco Discovery Protocol (CDP) and trusts the CoS that are received from the telephone. yword on the ports that are connected to the interior of the network. Because it is traffic has already been classified by the other edge devices, the CoS/DSCP labels in				
sage Guidelines	QoS domain inc incoming traffic Use the cisco-pl phones. The swi labels in packets Use the trust ke assumed that the these packets are	ludes the switch, the interior of the network, and the edge devices that can classify for QoS. none keyword on the ports at the edge of the network that are connected to Cisco IP tch detects the telephone through the Cisco Discovery Protocol (CDP) and trusts the CoS that are received from the telephone. yword on the ports that are connected to the interior of the network. Because it is traffic has already been classified by the other edge devices, the CoS/DSCP labels in				
sage Guidelines	QoS domain inc incoming traffic Use the cisco-pl phones. The swi labels in packets Use the trust ke assumed that the these packets are When you enabl	ludes the switch, the interior of the network, and the edge devices that can classify for QoS. none keyword on the ports at the edge of the network that are connected to Cisco IP tch detects the telephone through the Cisco Discovery Protocol (CDP) and trusts the CoS that are received from the telephone. yword on the ports that are connected to the interior of the network. Because it is traffic has already been classified by the other edge devices, the CoS/DSCP labels in trusted.				
sage Guidelines	QoS domain inc incoming traffic Use the cisco-pl phones. The swi labels in packets Use the trust ke assumed that the these packets are When you enabl • QoS is glob	 ludes the switch, the interior of the network, and the edge devices that can classify for QoS. none keyword on the ports at the edge of the network that are connected to Cisco IP tch detects the telephone through the Cisco Discovery Protocol (CDP) and trusts the Cost that are received from the telephone. word on the ports that are connected to the interior of the network. Because it is a traffic has already been classified by the other edge devices, the CoS/DSCP labels in the trusted. e the auto-QoS feature on the specified interface, these actions automatically occur: 				

• 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 that is 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 that are received in the incoming packets when the switch or router that is 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 that are 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 gos voip cisco-phone
```

This example shows how to display the QoS configuration that is automatically generated when auto-QoS is enabled on an interface on Supervisor Engines other than a Supervisor Engine 6-E:

```
Switch# debug auto gos
AutoQoS debugging is on
Switch# configure 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:gos
00:00:57:gos map cos 3 to dscp 26
00:00:57:gos map cos 5 to dscp 46
00:00:58:qos map dscp 32 to tx-queue 1
00:00:58:gos dbl
00:01:00:policy-map autoqos-voip-policy
00:01:00: class class-default
00:01:00:
           db]
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 gos voip cisco-phone
Switch(config-if)#
00:00:55:gos
00:00:56:qos map cos 3 to dscp 26
00:00:57:gos map cos 5 to dscp 46
00:00:58:gos map dscp 32 to tx-gueue 1
00:00:58:qos dbl
00:00:59:policy-map autoqos-voip-policy
```

L

```
00:00:59: class class-default
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
```

This example shows how to display the QoS configuration that is automatically generated when auto-QoS is enabled on an interface on a Supervisor Engine 6-E:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface gigabitethernet3/10
Switch(config-if) #auto qos voip trust
Switch(config-if)#
1d03h: service-policy input AutoQos-VoIP-Input-Cos-Policy
1d03h: service-policy output AutoQos-VoIP-Output-Policy
Switch(config-if)#intface gigabitethernet3/11
Switch(config-if)#auto gos voip
cisco-phone
Switch(config-if)#
1d03h: gos trust device cisco-phone
1d03h: service-policy input AutoQos-VoIP-Input-Cos-Policy
1d03h: service-policy output AutoQos-VoIP-Output-Policy
Switch(config-if)#end
Switch#
```

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

Related Commands	Command	Description
	debug auto qos (refer to Cisco IOS documentation)	Debugs Auto QoS.
	qos map cos	Defines the ingress CoS-to-DSCP mapping for the trusted interfaces.
	qos trust	Sets the trusted state of an interface.
	show auto qos	Displays the automatic quality of service (auto-QoS) configuration that is applied.
	show qos	Displays QoS information.
	show qos interface	Displays queueing information.
	show qos maps	Displays QoS map information.

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 automa	tic synchronization of all configuration files
Command Modes	Redundancy main	n-cpu
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	If you enter the n	no auto-sync standard command, no automatic synchronizations occur.
Examples		ows how (from the default configuration) to enable automatic synchronization of the gister 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		

bandwidth

To specify or modify the minimum bandwidth provided to a class belonging to a policy map attached to a physical port, use the **bandwidth** policy-map class command. To return to the default setting, use the **no** form of this command.

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

no bandwidth

Syntax Description		
oyntax bescription	bandwidth-kbps	Amount of bandwidth in kbps assigned to the class. The range is 32 to 16000000.
	percent percent	Percentage of available bandwidth assigned to the parent class. The range is 1 to 100.
	remaining percent percent	Percentage of remaining bandwidth assigned to parent class. The range is 1 to 100. This command is supported only when priority queuing class is configured, and the prioity queuing class is not rate-limited.
Defaults	No bandwidth is specified.	
Command Modes	Policy-map class configurat	ion
Command History	Release M	lodification
Command History	12.2(40)SG T	Indification his command was introduced on the Catalyst 4500 series switch using a upervisor Engine 6E.
Command History Usage Guidelines	12.2(40)SG TI Su	his command was introduced on the Catalyst 4500 series switch using a
	12.2(40)SG The bandwidth command sp	his command was introduced on the Catalyst 4500 series switch using a upervisor Engine 6E.
	12.2(40)SGThe second secon	his command was introduced on the Catalyst 4500 series switch using a upervisor Engine 6E. nd only in a policy map attached to a physical port. pecifies the minimum bandwidth for traffic in that class when there is traffic

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

- If the **percent** keyword is used, the sum of the class bandwidth percentages within a single policy map cannot exceed 100 percent. Percentage calculations are based on the bandwidth available on the port.
- The amount of bandwidth configured should be large enough to accommodate Layer 2 overhead.
- A policy map can have all the class bandwidths specified in either kbps or in percentages, but not a mix of both.

Examples

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

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map polmap6
Switch(config-pmap)# class silver-class
Switch(config-pmap-c)# bandwidth 2000
Switch(config-pmap-c)# end
```

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

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# bandwidth percent 25
Switch(config-pmap-c)# bandwidth percent 25
Switch(config-pmap-c)# exit
Switch(config-pmap)# end
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy input policy1
Switch(config-if)# end
```

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

```
Switch# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map policy1
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# bandwidth remaining percent 25
Switch(config-pmap-c)# bandwidth remaining percent 25
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# end
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# end
```

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

L

Command	Description
class	Specifies the name of the class whose traffic policy you want to create or change.
dbl	Enables active queue management on a transmit queue used by a class of traffic.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
priority	Enables the strict priority queue (low-latency queueing [LLQ]) and to give priority to a class of traffic belonging to a policy map attached to a physical port.
service-policy (policy-map class)	Creates a service policy that is a quality of service (QoS) policy within a policy map.
shape (class-based queueing)	Enables traffic shaping a class of traffic in a policy map attached to a physical port.
show policy-map	Displays information about the policy map.

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 config	zuration mode	
Command Modes	Interface config		
	Release	Modification	
	Release 12.1(8a)EW	Modification Support for this command was introduced on the Catalyst 4500 series switch.	
Command Modes Command History	Release	Modification	
Command History	Release 12.1(8a)EW 12.1(13)EW You do not have group. If a port-	Modification Support for this command was introduced on the Catalyst 4500 series switch.	
Command History	Release12.1(8a)EW12.1(13)EWYou do not have group. If a port- interface for the If a specific character	Modification Support for this command was introduced on the Catalyst 4500 series switch. Support for LACP was added. e to create a port-channel interface before assigning a physical interface to a channel other interface has not been created, it is automatically created when the first physical	
	Release 12.1(8a)EW 12.1(13)EW You do not have group. If a port- interface for the If a specific cha channel number versa. You can also cr Layer 3 port cha command befor	Modification Support for this command was introduced on the Catalyst 4500 series switch. Support for LACP was added. e to create a port-channel interface before assigning a physical interface to a channel -channel interface has not been created, it is automatically created when the first physica e channel group is created. annel number is used for the PAgP-enabled interfaces of a channel group, that same	

	interfaces within the same chann	anges that you make to the port-channel interface are propagated to all el group as the port channel (for example, configuration changes are iterfaces that are not part of the port channel, but are part of the channel	
	ble EtherChannel by connecting two port groups together.		
<u> </u>	Do not enable Layer 3 addresses on the physical EtherChannel interfaces. Do not assign bridge groon the physical EtherChannel interfaces because it creates loops.		
Examples	This example shows how to add specified by port-channel 45:	Gigabit Ethernet interface 1/1 to the EtherChannel group that is	
	Switch(config-if)# channel-g Creating a port-channel inter Switch(config-if)#	-	
Related Commands	Command	Description	
	interface port-channel	Accesses or creates a port-channel interface.	
	show interfaces port-channel (refer to Cisco IOS documentation)	Displays the information about the Fast EtherChannel.	

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			
Domano	PAgP			
Command Modes	Interface configuration mode			
Command History	Release	Modification		
	12.1(13)EV	V Support for this command was introduced on the Catalyst 4500 series switches.		
Usage Guidelines	This comma	and is not supported on systems that are configured with a Supervisor Engine I.		
	You can also select the protocol using the channel-group command.			
	If the interf	ace 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 L	ACP are not compatible; both ends of a channel must use the same protocol.		
	You can ma	nually 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 a for LACP m	ll ports in an EtherChannel to operate at the same speed and duplex mode (full duplex only node).		
		ete list of guidelines, refer to the "Configuring EtherChannel" section of the Catalyst 4500 ch Cisco IOS Software Configuration Guide.		
Examples	-	le shows how to select LACP to manage channeling on the interface: fig-if) # channel-protocol lacp		
	Switch(con Switch(con			

Related Commands	Command	Description
	channel-group	Assigns and configures an EtherChannel interface to an EtherChannel group.
	show etherchannel	Displays EtherChannel information for a channel.

class

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

class class-name

no class class-name

Syntax Description	class-name	Name of the predefined traffic class for which you want to configure or modify a	
		traffic policy. The class was previously created through the class-map <i>class-map-name</i> global configuration command.	
Defaults	No classes are	defined; except for the class-default.	
Command Modes	Policy-map con	nfiguration	
Command History	Release	Modification	
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switches.	
Usage Guidelines	the class-map command to id policy map, you classes in that p ties the charact configured three by using the se	the class command, you must create a class map for matching packets to the class by using global configuration command. You also must use the policy-map global configuration entify the policy map and to enter policy-map configuration mode. After specifying a u can configure a traffic policy for new classes or modify a traffic policy for any existing policy map. The class name that you specify with the class command in the policy map eristics for that class—that is, its policy—to the class map and its match criteria, as ough the class-map global configuration command. You attach the policy map to a port rvice-policy (interface configuration) configuration command.	
	After you enter the class command, the switch enters policy-map class configuration mode, and these configuration commands are available:		
	• bandwidth : specifies or modifies the minimum bandwidth provided to a class belonging to a policy map. For more information, see the bandwidth command. This command is only available on the Supervisor Engine 6-E and Catalyst 4900M chassis.		
		es dynamic buffer limiting for traffic hitting this class. For details on dbl parameters refer v qos dbl command.	
	• exit: exits policy-map class configuration mode and returns to policy-map configuration mode.		
	• no : returns a command to its default setting.		
	the commi	figures a single-rate policer, an aggregate policer, or a two-rate traffic policer that uses tted information rate (CIR) and the peak information rate (PIR) for a class of traffic. The ecifies the bandwidth limitations and the action to take when the limits are exceeded. For	

more information, see the police command. For more information about the two-rate policer, see the **police (two rates)** and the **police (percent)** command. The two rate traffic policer is supported on a Supervisor Engine 6-E and Catalyst 4900M chassis.

- **priority**: enables the strict priority queue for a class of traffic. For more information, see the **priority** command. This command is effective on a Supervisor Engine 6-E and Catalyst 4900M chassis.
- **service-policy (policy-map class)**: creates a service policy as a quality of service (QoS) policy within a policy map (called a hierarchical service policy). For more information, see the **service-policy (policy-map class)** command. This command is effective only in a hierarchical policy map attached to an interface.
- set: classifies IP traffic by setting a class of service (CoS), a Differentiated Services Code Point (DSCP) or IP-precedence in the packet. For more information, see the set command.
- shape (class-based queueing): sets the token bucket committed information rate (CIR) in a policy map. For more information, see the shape (class-based queueing) command. This command is effective on a Supervisor Engine 6-E and Catalyst 4900M chassis.
- **trust**: defines a trust state for a traffic class. For more information, see the **trust** command. This command is not supported on a Supervisor Engine 6-E and Catalyst 4900M chassis.

The switch supports up to 256 classes, including the default class, in a policy map. Packets that fail to meet any of the matching criteria are classified as members of the default traffic class. You configure the default traffic class by specifying **class-default** as the class name in the **class** policy-map class configuration command. You can manipulate the default traffic class (for example, set policies to police or to shape it) just like any other traffic class, but you cannot delete it.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Examples

This example shows how to create a policy map called *policy1*. When attached to an ingress port, the policy matches all the inbound traffic defined in *class1*, sets the IP DSCP to 10, and polices the traffic at an average rate of 1 Mbps and bursts of 20 KB. Traffic exceeding the profile is marked down to a Traffic exceeding the profile is marked down to a DSCP value obtained from the policed-DSCP map and then sent.

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

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

Related Commands	Command	Description
	bandwidth	Specifies or modifies the minimum bandwidth provided to a class belonging to a policy map attached to a physical port.
	class-map	Creates a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode.
	dbl	Enables active queue management on a transmit queue used by a class of traffic.
	police	Configures the Traffic Policing feature.
	police (percent)	Configures traffic policing on the basis of a percentage of bandwidth available on an interface.
	police rate	Configures single- or dual-rate policer.
	policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
	priority	Enables the strict priority queue (low-latency queueing [LLQ]) and to give priority to a class of traffic belonging to a policy map attached to a physical port.
	service-policy (interface configuration)	Attaches a policy map to an interface.
	service-policy (policy-map class)	Creates a service policy that is a quality of service (QoS) policy within a policy map.
	set	Marks IP traffic by setting a class of service (CoS), a Differentiated Services Code Point (DSCP), or IP-precedence in the packet.
	shape (class-based queueing)	Enables traffic shaping a class of traffic in a policy map attached to a physical port.
	show policy-map	Displays information about the policy map.
	trust	Defines a trust state for traffic classified through the class policy-map configuration command.

class-map

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

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

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

criteria in the class map must be matched. match-any (Optional) Perform a logical-OR of the matching statements under map. One or more criteria in the class map must be matched. class-map-name Name of the class map. Defaults No class maps are defined. If neither the match-all nor the match-any keyword is specified, the default is match-all Command Modes Global configuration Command History Release Modification 12.1(8a)EW Support for this command was introduced on the Catalyst 4500 series sw Usage Guidelines Use this command to specify the name of the class for which you want to create or modifiguration match criteria and to enter class-map configuration mode. Packets are checked against the reconfigured for a class map to decide if the packet belongs to that class. If a packet matches criteria, the packet is considered a member of the class and is forwarded according to the service (QoS) specifications set in the traffic policy. After you enter the class-map command, the switch enters class-map configuration mode configuration commands are available: description: describes the class map (up to 200 characters). The show class-map priv command displays the description and the name of the class map. exit: exits from QoS class-map configuration mode. match: configures classification criteria. For more information, see the match (class configuration) command. 					
map. One or more criteria in the class map must be matched. class-map-name Name of the class map. Defaults No class maps are defined. If neither the match-all nor the match-any keyword is specified, the default is match-all Command Modes Global configuration Command History Release Modification 12.1(8a)EW Support for this command was introduced on the Catalyst 4500 series sw Use this command to specify the name of the class for which you want to create or modifi match criteria and to enter class-map configuration mode. Packets are checked against the resorties of a class map to decide if the packet belongs to that class. If a packet matches criteria, the packet is considered a member of the class and is forwarded according to the service (QoS) specifications set in the traffic policy. After you enter the class-map comfiguration mode. • After you enter the class-map configuration mode configuration commands are available: • description: describes the class map (up to 200 characters). The show class-map priv command displays the description and the name of the class map. • exit: exits from QoS class-map configuration mode. • match: configures classification criteria. For more information, see the match (class configuration) command.	Syntax Description	match-all	(Optional) Perform a logical-AND of all matching under this class map. All criteria in the class map must be matched.		
Defaults No class maps are defined. If neither the match-all nor the match-any keyword is specified, the default is match-all Command Modes Global configuration Release Modification 12.1(8a)EW Support for this command was introduced on the Catalyst 4500 series sw Usage Guidelines Use this command to specify the name of the class for which you want to create or modifimatch criteria and to enter class-map configuration mode. Packets are checked against the reconfigured for a class map to decide if the packet belongs to that class. If a packet matches criteria, the packet is considered a member of the class and is forwarded according to the service (QoS) specifications set in the traffic policy. After you enter the class-map command, the switch enters class-map configuration mode configuration commands are available: description: describes the class map (up to 200 characters). The show class-map priv command displays the description and the name of the class map. exit: exits from QoS class-map configuration mode. match: configures classification criteria. For more information, see the match (class configuration) command. 		match-any	(Optional) Perform a logical-OR of the matching statements under this class map. One or more criteria in the class map must be matched.		
If neither the match-all nor the match-any keyword is specified, the default is match-all Command Modes Global configuration Command History Release Modification 12.1(8a)EW Support for this command was introduced on the Catalyst 4500 series sw Usage Guidelines Use this command to specify the name of the class for which you want to create or modify match criteria and to enter class-map configuration mode. Packets are checked against the r configured for a class map to decide if the packet belongs to that class. If a packet matches criteria, the packet is considered a member of the class and is forwarded according to the service (QoS) specifications set in the traffic policy. After you enter the class-map command, the switch enters class-map configuration mode configuration commands are available: • description: describes the class map (up to 200 characters). The show class-map priv command displays the description and the name of the class map. • exit: exits from QoS class-map configuration mode. • match: configures classification criteria. For more information, see the match (class configuration) command.		class-map-name	Name of the class map.		
Command Modes Global configuration Command History Release Modification 12.1(8a)EW Support for this command was introduced on the Catalyst 4500 series sw Usage Guidelines Use this command to specify the name of the class for which you want to create or modifimatch criteria and to enter class-map configuration mode. Packets are checked against the reconfigured for a class map to decide if the packet belongs to that class. If a packet matches criteria, the packet is considered a member of the class and is forwarded according to the service (QoS) specifications set in the traffic policy. After you enter the class-map command, the switch enters class-map configuration mode configuration commands are available: description: describes the class map (up to 200 characters). The show class-map priv command displays the description and the name of the class map. exit: exits from QoS class-map configuration mode. match: configures classification criteria. For more information, see the match (class configuration) command. 	Defaults	No class maps are	e defined.		
Command History Release Modification 12.1(8a)EW Support for this command was introduced on the Catalyst 4500 series sw Usage Guidelines Use this command to specify the name of the class for which you want to create or modifimatch criteria and to enter class-map configuration mode. Packets are checked against the right configured for a class map to decide if the packet belongs to that class. If a packet matches criteria, the packet is considered a member of the class and is forwarded according to the service (QoS) specifications set in the traffic policy. After you enter the class-map command, the switch enters class-map configuration mode configuration commands are available: • description: describes the class map (up to 200 characters). The show class-map priv command displays the description and the name of the class map. • exit: exits from QoS class-map configuration mode. • match: configures classification criteria. For more information, see the match (class configuration) command.		If neither the match-all nor the match-any keyword is specified, the default is match-all .			
12.1(8a)EW Support for this command was introduced on the Catalyst 4500 series sw Usage Guidelines Use this command to specify the name of the class for which you want to create or modify match criteria and to enter class-map configuration mode. Packets are checked against their configured for a class map to decide if the packet belongs to that class. If a packet matches criteria, the packet is considered a member of the class and is forwarded according to the service (QoS) specifications set in the traffic policy. After you enter the class-map command, the switch enters class-map configuration mode configuration commands are available: description: describes the class map (up to 200 characters). The show class-map prive command displays the description and the name of the class map. exit: exits from QoS class-map configuration mode. match: configures classification criteria. For more information, see the match (class-configuration) command. 	Command Modes	Global configurat	ion		
 Use this command to specify the name of the class for which you want to create or modify match criteria and to enter class-map configuration mode. Packets are checked against the right configured for a class map to decide if the packet belongs to that class. If a packet matches criteria, the packet is considered a member of the class and is forwarded according to the service (QoS) specifications set in the traffic policy. After you enter the class-map command, the switch enters class-map configuration mode configuration commands are available: description: describes the class map (up to 200 characters). The show class-map priv command displays the description and the name of the class map. exit: exits from QoS class-map configuration mode. match: configures classification criteria. For more information, see the match (class-configuration) command. 	Command History	Release M	Modification		
 match criteria and to enter class-map configuration mode. Packets are checked against the reconfigured for a class map to decide if the packet belongs to that class. If a packet matches criteria, the packet is considered a member of the class and is forwarded according to the service (QoS) specifications set in the traffic policy. After you enter the class-map command, the switch enters class-map configuration mode configuration commands are available: description: describes the class map (up to 200 characters). The show class-map priv command displays the description and the name of the class map. exit: exits from QoS class-map configuration mode. match: configures classification criteria. For more information, see the match (class configuration) command. 		12.1(8a)EW S	Support for this command was introduced on the Catalyst 4500 series switches.		
 configuration commands are available: description: describes the class map (up to 200 characters). The show class-map priv command displays the description and the name of the class map. exit: exits from QoS class-map configuration mode. match: configures classification criteria. For more information, see the match (class configuration) command. 	Usage Guidelines	match criteria and configured for a cl criteria, the packe	I to enter class-map configuration mode. Packets are checked against the match criteria lass map to decide if the packet belongs to that class. If a packet matches the specified et is considered a member of the class and is forwarded according to the quality of		
 command displays the description and the name of the class map. exit: exits from QoS class-map configuration mode. match: configures classification criteria. For more information, see the match (class-configuration) command. 		After you enter the class-map command, the switch enters class-map configuration mode, and these configuration commands are available:			
• match: configures classification criteria. For more information, see the match (class- configuration) command.		• description : describes the class map (up to 200 characters). The show class-map privileged EXEC command displays the description and the name of the class map.			
configuration) command.		• exit: exits from QoS class-map configuration mode.			
• not removes a match statement from a class mon					
• no: removes a match statement from a class map.		• no : removes a	a match statement from a class map.		

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

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

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

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

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

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

clear counters

To clear the 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							
Syntax Description	FastEthernet interface_number GigabitEthernet interface_number		(Optional) Specifies the Fast Ethernet interface; valid values are from 1 to 9.				
			(Optional) Specifies the Gigabit Ethernet interface; valid values are from 1 to 9.				
	null interface_num	nber	(Optional) Specifies the null interface; the valid value is 0.				
	port-channel nun	ıber	(Optional) Specifies the channel interface; valid values are from 1 to 64.				
	vlan vlan_id	vlan_id(Optional) Specifies the VLAN; valid values are from 1 to 4096.					
Defaults	This command has	no default settings	ş.				
Command Modes	Privileged EXEC	node					
Command History	Release	Modification					
	12.1(8a)EW Support for this command was introduced on the Catalyst 4500 series switch.						
	12.1(0a)Ew	Support for this c	ommand was introduced on the Catalyst 4500 series switch.				
	12.1(8a)EW 12.1(12c)EW		ded VLAN addresses was added.				
Usage Guidelines	12.1(12c)EW This command cle	Support for exten					
Usage Guidelines	12.1(12c)EW	Support for exten	ded VLAN addresses was added.				
Usage Guidelines Note	12.1(12c)EW This command cle interface. This command doe	Support for exten	ded VLAN addresses was added. nterface counters from all the interfaces unless you specify an nters that are retrieved using SNMP, but only those seen when you				
Note	12.1(12c)EW This command cle interface. This command doe enter the show int	Support for exten ars all the current i es not clear the cour erface counters co	ded VLAN addresses was added. nterface counters from all the interfaces unless you specify an nters that are retrieved using SNMP, but only those seen when you				
	12.1(12c)EW This command cle interface. This command doe enter the show int This example show Switch# clear co	Support for exten ars all the current i es not clear the cour erface counters co vs how to clear all t unters	ded VLAN addresses was added. nterface counters from all the interfaces unless you specify an nters that are retrieved using SNMP, but only those seen when you mmand.				
Note	12.1(12c)EW This command cle interface. This command doe enter the show int This example show Switch# clear co Clear "show inte Switch#	Support for exten ars all the current i es not clear the cour erface counters co vs how to clear all t unters rface" counters c	ded VLAN addresses was added. nterface counters from all the interfaces unless you specify an nters that are retrieved using SNMP, but only those seen when you mmand.				

Related Commands	Command	Description	
	show interface counters (refer	Displays interface counter information.	
	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	slot_num	Slot on a line module.
Defaults	The password	is not cleared.
Command Modes	Privileged EXI	EC mode
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 s	shows how to clear the password from slot 5 on a line module:
	Switch# clear Switch#	hw-module slot 5 password
Related Commands	Command	Description
	hw-module p	ower Turns the power off on a slot or line module.

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 mod/port

Syntax Description	<i>mod/port</i> Number of the module and port.				
Defaults	This command l	has no default settings.			
Command Modes	Privileged EXEC mode				
Command History	Release	Modification			
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.			
Examples	This example sh	nows how to clear the hardware logic from a Gigabit Ethernet IEEE 802.3z interface:			
	Switch# clear Switch#	interface gigabitethernet 1/1			
Related Commands	Command	Description			
	show interface	s status Displays the interface status.			

clear interface vlan

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

clear interface vlan number

Syntax Description	number Nu	mber of the VLAN interface; valid values are from 1 to 4094.
Defaults	This command h	as no default settings.
Command Modes	Privileged EXE	C mode
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	-	ows how to clear the hardware logic from a specific VLAN:
	Switch#	
Related Commands	Command	Description
	show interface	s status Displays the interface status.
clear ip access-template

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

clear ip access-template access-list

Syntax Description	access-list	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	l has no default settings.
Command Modes	Privileged EX	EC mode
Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Examples	-	shows how to clear the statistical information for an access list:

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

- **Defaults** This command has no default settings.
- **Command Modes** Privileged EXEC mode

 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	Command	Description
	arp access-list	Defines an ARP access list or adds clauses at the end of a predefined list.
	show ip arp inspection log	Displays the status of the log buffer.

clear ip arp inspection statistics

show ip arp inspection log

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 vlan	e-range	(Optional) Spe	cifies the VLAN r	ange.	
Defaults	This com	mand has no de	fault settings.			
Command Modes	Privileged	I EXEC mode				
Command History	Release Modification					
	12.1(19)E	EW Suppo	ort for this comm	and was introduce	ed on the Ca	talyst 4500 series switch.
Examples		-			LAN 1 and 1	how to verify the removal:
Examples	Switch# c Switch# s Vlan	zlear ip arp i show ip arp ir Forwarded	Inspection stat : Aspection stati Dropped	istics vlan 1 stics vlan 1 DHCP Drops	ACL Dro	ps
Examples	Switch# c Switch# s Vlan 1	clear ip arp i show ip arp ir Forwarded 0	Inspection stat: Aspection static Dropped 0	istics vlan 1 stics vlan 1 DHCP Drops 0	ACL Dro	ps
Examples	Switch# c Switch# s Vlan 1 Vlan I	clear ip arp i show ip arp ir Forwarded 	Anspection stat: aspection static Dropped 0 ACL Permits 	istics vlan 1 stics vlan 1 DHCP Drops	ACL Dro	ps
Examples	Switch# c Switch# s Vlan 1 Vlan I	clear ip arp i show ip arp ir Forwarded 0 DHCP Permits	Anspection stat: aspection static Dropped 0 ACL Permits	istics vlan 1 stics vlan 1 DHCP Drops 0 Source MAC Fai	ACL Dro	ps
Examples	Switch# c Switch# s Vlan 1 Vlan I 1	clear ip arp i show ip arp ir Forwarded 	Anspection stat: aspection static Dropped 0 ACL Permits 0 ures IP Valida	istics vlan 1 stics vlan 1 DHCP Drops 0 Source MAC Fai	ACL Dro	ps
Examples	Switch# c Switch# s Vlan Vlan I 1 Vlan I	clear ip arp i show ip arp ir Forwarded 	Anspection stat: aspection static Dropped 0 ACL Permits 0 ures IP Valida	istics vlan 1 stics vlan 1 DHCP Drops 	ACL Dro	ps
	Switch# c Switch# s Vlan 1 Vlan 1 1 Vlan 1 1 Vlan 1 1	clear ip arp i show ip arp ir Forwarded 	Anspection stat: aspection static Dropped 0 ACL Permits 0 ares IP Valida	istics vlan 1 stics vlan 1 DHCP Drops 0 Source MAC Fai 	ACL Dro	ps
Examples	Switch# c Switch# s Vlan 1 Vlan I 1 Vlan I 1 Switch#	clear ip arp i show ip arp ir Forwarded 	Anspection stat: Dropped 0 ACL Permits 0 Dropped 0 ACL Permits 0 Descrip Defines	istics vlan 1 stics vlan 1 DHCP Drops 0 Source MAC Fai ation Failures 0 0	ACL Dro	ps

Displays the status of the log buffer.

clear ip dhcp snooping binding

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

clear ip dhcp snooping binding [*] [ip-address] [vlan vlan_num] [interface interface_num]

Syntax Description	*	(Optional) clearing all DHCP snooping binding entries.		
	ip-address	(Optional) IP address for the DHCP snooping binding entries		
	vlan vlan_num	(Optional) Specifies a VLAN.		
	interface interface_num	(Optional) Specifies an interface.		
Defaults	This command has no defa	ault settings.		
Command Modes	Privileged EXEC			
Command History	Release	Modification		
	12.2(44)SG	Support for this command was introduced on the Catalyst 4500 series switch.		
Usage Guidelines		ly used to clear DHCP snooping binding entries. d on a VLAN only if both the global snooping and the VLAN snooping are		
Examples	This example shows how t Switch#clear ip dhcp sn Switch#	to clear all the DHCP snoop binding entries:		
	This example shows how to clear a specific DHCP snoop binding entry:			
	Switch#clear ip dhcp snooping binding 1.2.3.4 Switch#			
	This example shows how to clear all the DHCP snoop binding entries on the GigabitEthernet interface 1/1:			
	Switch#clear ip dhcp snooping binding interface gigabitEthernet 1/1 Switch#			
	This example shows how to clear all the DHCP snoop binding entries on VLAN 40:			
	Switch#clear ip dhcp snooping binding vlan 40 Switch#			

Related Commands C

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping binding	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

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 mode

 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	Command	Description
	ip dhcp snooping	Globally enables DHCP snooping.
	ip dhcp snooping binding	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
	ip dhcp snooping information option	Enables DHCP option 82 data insertion.
	ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
	ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
	show ip dhcp snooping	Displays the DHCP snooping configuration.
	show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

clear ip dhcp snooping database statistics

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

clear ip dhcp snooping database statistics

Defaults This command has no default setting

Command Modes Privileged EXEC mode

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	Command	Description
	ip dhcp snooping	Globally enables DHCP snooping.
	ip dhcp snooping binding	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
	ip dhcp snooping information option	Enables DHCP option 82 data insertion.
	ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
	ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
	show ip dhcp snooping	Displays the DHCP snooping configuration.
	show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

clear ip igmp group

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

clear ip igmp group [{fastethernet mod/port} | {GigabitEthernet mod/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.
	mod/port	(Optional) Number of the module and port.
	GigabitEthernet	(Optional) Specifies the Gigabit Ethernet interface.
	host_name	(Optional) Hostname, as defined in the DNS hosts table or with the
		ip host command.
	group_address	(Optional) Address of the multicast group in four-part, dotted notation.
	Loopback interface_number	(Optional) Specifies the loopback interface; valid values are from 0 to 2,147,483,647.
	null interface_number	(Optional) Specifies the null interface; the valid value is 0.
	port-channel number	(Optional) Specifies the channel interface; valid values are from 1 to 64.
	vlan vlan_id	(Optional) Specifies the VLAN; valid values are from 1 to 4094.
Command Modes Command History	Privileged EXEC mode Release Modification	
Gommanu mistory		
		r this command was introduced on the Catalyst 4500 series switch.
Usage Guidelines		r this command was introduced on the Catalyst 4500 series switch.
Usage Guidelines	The IGMP cache contains a li are members.	·
Usage Guidelines Examples	The IGMP cache contains a li are members. To delete all the entries from t arguments.	st of the multicast groups of which hosts on the directly connected LAN

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

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

Related Commands C

Command	Description
ip host (refer to Cisco IOS documentation)	Defines a static host name-to-address mapping in the host cache.
show ip igmp groups (refer to Cisco IOS documentation)	Displays the multicast groups with receivers that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP), use the show ip igmp groups command in EXEC mode.
show ip igmp interface	Displays the information about the IGMP-interface status and configuration.

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 vlan_id	(Optional) Specifies a VI	AN; valid values are from 1 to 1001 and from 1006 to 4094.
Defaults	This command	has no default settings.	
Command Modes	Privileged EXEC mode		
Command History	Release	Modification	
	12.1(20)EW	Support for this comma	nd 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 the IGMP snooping statistics for VLAN 25:		
	Switch# clear ip igmp snooping membership vlan 25 Switch#		ship vlan 25
Related Commands	Command		Description
	ip igmp snoopi	ng vlan explicit-tracking	Enables per-VLAN explicit host tracking.
	show ip igmp s	snooping membership	Displays host membership information.

clear ip mfib counters

To clear the global MFIB counters and the 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 ha	s no default settings.
----------	-----------------	------------------------

Command Modes Privileged EXEC mode

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	Command	Description
	show ip mfib	Displays all active Multicast Forwarding Information Base (MFIB) routes.

clear ip mfib fastdrop

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

clear ip mfib fastdrop

Syntax Description	This command has no arguments or keywords.
σγικάλ μεσυτιριτοπ	This command has no arguments of keywords.

- **Defaults** This command has no default settings.
- **Command Modes** Privileged EXEC mode

 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, the new fast-drop entries are created.

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

Switch# **clear ip mfib fastdrop** Switch#

Related Commands	Command	Description
	ip mfib fastdrop	Enables MFIB fast drop.
	show ip mfib fastdrop	Displays all currently active fast-drop entries and shows whether fast drop is enabled.

clear lacp counters

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

clear lacp [channel-group] counters

Syntax Description	channel-group	(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 Catalyst 4500 series switches.	
Usage Guidelines	This command is not supported on systems that are configured with a Supervisor Engine I. If you do not specify a channel group, all channel groups are cleared. If you enter this command for a channel group that contains members in PAgP mode, the corignored.		
Examples	This example sho Switch# clear I Switch#	ows how to clear the statistics for a specific group: Lacp 1 counters	
Related Commands	Command show lacp	Description Displays LACP information.	

clear mac-address-table

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

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

Syntax Description	dynamic	Specifies dynamic entry types.
Syntax Description	•	
	address mac_addr	(Optional) Specifies the MAC address.
	interface interface	(Optional) Specifies the interface and clears the entries associated with it; valid values are FastEthernet and GigabitEthernet .
	vlan vlan_id	(Optional) Specifies the VLANs; valid values are from 1 to 4094.
	notification	Specifies MAC change notification global counters.
Defaults	This command has n	o default settings.
Command Modes	Privileged EXEC mode	
Command History	Release M	odification
	12.1(8a)EW Su	upport for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW Su	apport for extended VLAN addresses added.
	12.2(31)SG Su	apport for MAC address notification global counters added.
Usage Guidelines	Enter the clear mac-a from the table.	address-table dynamic command with no arguments to remove all dynamic entries
	The clear mac-address-table notification command only clears the global counters which are displayed with show mac-address-table notification command. It does not clear the global counters and the history table of the CISCO-MAC-NATIFICATION-MIB.	
Examples	This example shows how to clear all the dynamic Layer 2 entries for a specific interface (gi1/1):	
	Switch# clear mac-address-table dynamic interface gi1/1 Switch#	
	This example shows	how to clear the MAC address notification counters:

Related Commands	Command	Description
	clear mac-address-table dynamic	Clears the dynamic address entries from the Layer 2 MAC address table.
	mac-address-table aging-time	Configures the aging time for entries in the Layer 2 table.
	mac-address-table notification	Enables MAC address notification on a switch.
	main-cpu	Enters the main CPU submode and manually synchronize the configurations on the two supervisor engines.
	show mac-address-table address	Displays the information about the MAC-address table.
	snmp-server enable traps	Enables SNMP notifications.

clear mac-address-table dynamic

To clear the 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 mac_addr	(Optional) Spec	ifies the MAC address.
	interface interface		ifies the interface and clears the entries associated with it; valid
	values are Fast		thernet and GigabitEthernet.
	vlan vlan_id	(Optional) Spec	ifies the VLANs; valid values are from 1 to 4094.
Defaults	This command has no	o default settings.	
Command Modes	Privileged EXEC mo	de	
Command History	Release M	odification	
	12.1(8a)EW Support for this command was introduced on the Catalyst 4500 series switch.		
	12.1(12c)EW Su	apport for extended	d VLAN addresses added.
Usage Guidelines	Enter the clear mac-a from the table.	address-table dyn	amic command with no arguments to remove all dynamic entries
Examples	This example shows	how to clear all the	e dynamic Layer 2 entries for a specific interface (gi1/1):
	Switch# clear mac-address-table dynamic interface gil/1 Switch#		
Related Commands	Command		Description
	mac-address-table a	aging-time	Configures the aging time for entries in the Layer 2 table.
	main-cpu		Enters the main CPU submode and manually synchronize the configurations on the two supervisor engines.
	show mac-address-	table address	Displays the information about the MAC-address table.

clear pagp

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

clear pagp {group-number | counters}

Syntax Description	group-number	Channel-group number; valid values are from 1 to 64.
- ,	counters	Clears traffic filters.
Defaults	This command ha	as no default settings.
ommand Modes	Privileged EXEC	mode
Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Examples	This example sho Switch# clear p Switch#	ows how to clear the port-channel information for a specific group:
	This example sho Switch# clear p Switch#	bws how to clear all the port-channel traffic filters:
Related Commands		
Related Commands	Command	Description

clear port-security

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

clear port-security dynamic [address mac-addr [vlan vlan-id]] | [interface interface-id] [vlan access | voice]

Syntax Description	dynamic	Deletes all the dynamic secure MAC addresses.	
eynax beeenpron	address mac-addr	(Optional) Deletes the specified secure MAC address.	
	vlan vlan-id	(Optional) Deletes the specified secure MAC address from the specified VLAN.	
	interface interface-id	(Optional) Deletes the secure MAC addresses on the specified physical port or port channel.	
	vlan access	(Optional) Deletes the secure MAC addresses from access VLANs.	
	vlan voice	(Optional) Deletes the secure MAC addresses from voice VLANs.	
Defaults	This command has no d	efault settings.	
command Modes	Privileged EXEC mode		
Jsage Guidelines	If you enter the clear port-security all command, the switch removes all the dynamic secure MAC addresses from the MAC address table. You can clear sticky and static secure MAC addresses one at a time with the no switchport port-security mac-address command.		
<u>Note</u>			
	If you enter the clear port-security dynamic interface <i>interface-id</i> command, the switch removes all the 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.	
	12.2(31)SG	Add support for sticky port security.	
Examples	This example shows how to remove all the dynamic secure addresses from the MAC address table:		
	This example shows how	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
---------	----------

Command	Description
show port-security	Displays information about the port-security setting.
switchport port-security	Enables port security on an interface.

clear qos

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

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

Syntax Description	aggregate-policer name	(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.	
	mod/interface	(Optional) Number of the module and interface.	
	vlan vlan_num	(Optional) Specifies a VLAN.	
	port-channel number	(Optional) Specifies the channel interface; valid values are from 1 to 64.	
Defaults	This command has no defa	ault settings.	
Command Modes	Privileged EXEC mode		
Command History	Release Modification		
	12.1(8a)EW Supp	ort for this command was introduced on the Catalyst 4500 series switch.	
Usage Guidelines <u>Note</u>	When you enter the clear	ported on the Supervisor Engine 6-E and Catalyst 4900M chassis. qos command, the way that the counters work is affected and the traffic that Id be forwarded for a short period of time.	
	-	esets the interface QoS policy counters. If no interface is specified, the clear ooS policy counters for all interfaces.	
Examples	This example shows how t protocols:	to clear the global and per-interface aggregate QoS counters for all the	
	Switch# clear qos Switch#		
	This example shows how t	to clear the specific protocol aggregate QoS counters for all the interfaces:	
	Switch# clear qos aggre Switch#	gate-policer	

Related Commands	Command	Description
	show qos	Displays QoS information.

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	vlan-id	(Optional) VLAN number; see the "Usage Guidelines" section for valid values.
Defaults	This command I	has no default settings.
Command Modes	Privileged EXE	C mode
Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switches.
Usage Guidelines	If you do not sp cleared.	ecify a <i>vlan-id</i> value; the software-cached counter values for all the existing VLANs are
Examples	This example sh	ows how to clear the software-cached counter values for a specific VLAN:
		vlan 10 counters an" counters on this vlan [confirm] y
Related Commands	Command	Description
	show vlan cour	nters Displays VLAN counter information.

clear vmps statistics

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

clear vmps statistics

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

Command Modes Privileged EXEC mode

Command HistoryReleaseModification12.1(13)EWSupport for this command was introduced on the Catalyst 4500 series switches.

 Examples
 This example shows how to clear the VMPS statistics:

 Switch# clear vmps statistics

 Switch#

Related Commands	Command	Description
	show vmps	Displays VMPS information.
	vmps reconfirm (privileged EXEC)	Changes the reconfirmation interval for the VLAN Query Protocol (VQP) client.

control-plane

To enter control-plane configuration mode, which allows users to associate or modify attributes or parameters (such as a service policy) that are associated with the control plane of the device, use the **control-plane** command.

control-plane

Syntax Description	This command has no arguments or keywords.		
Defaults	Default service police named "system-cpp-policy" is attached.		
Command Modes	Global configuration mode		
Command History	ReleaseModification12.2(31)SGSupport for this command was introduced.		
Usage Guidelines	This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.		
Note	You must set a policy action for every class. If you do not set a policy action for every class, the traffic skips the class that does not have a policy action and matches against the subsequent classes. After you enter the control-plane command, you can define control plane services for your route processor. For example, you can associate a service policy with the control plane to police all traffic that is destined to the control plane.		
Examples	These examples show how to configure trusted hosts with source addresses 10.1.1.1 and 10.1.1.2 to forward Telnet packets to the control plane without constraint, while allowing all remaining Telnet packets to be policed at the specified rate:		
	<pre>Switch(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet ! Allow 10.1.1.2 trusted host traffic. Switch(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet ! Rate limit all other Telnet traffic. Switch(config)# access-list 140 permit tcp any any eq telnet ! Define class-map "telnet-class." Switch(config)# class-map telnet-class Switch(config-cmap)# match access-group 140 Switch(config-map)# exit Switch(config-pmap)# class telnet-class Switch(config-pmap)# class telnet-class Switch(config-pmap)# class telnet-class Switch(config-pmap)# exit Switch(config-pmap)# exit L Define aggregate control plane service for the active Route Processor.</pre>		

Switch(config)# macro global apply system-cpp Switch(config)# control-plane Switch(config-cp)# service-police input system-cpp-policy Switch(config-cp)# exit

Command	Description
class	Specifies the name of the class whose traffic policy you want to create or change.
class-map	Creates a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode.
match access-group (refer to the Cisco IOS Release 12.2 Command Reference)	Configures the match criteria for a class map on the basis of the specified access control list (ACL).
policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
service-policy (interface configuration)	Attaches a policy map to an interface.
show policy-map control-plane	Displays the configuration either of a class or of all classes for the policy map of a control plane.

counter

To assign a counter set to a switch port, use the **counter** command. To remove a counter assignment, use the no form of this command.

counter

no counter

- **Syntax Description** This command has no arguments or keywords.
- **Defaults** This command has no default setting.
- **Command Modes** Interface configuration mode

Command History	Release	Modification
	12.2(40)SG	Support for this command was introduced.

Usage GuidelinesThis command is supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.
The total number of switch ports that can have transmit and receive counters is 4096.
When a Layer 3 port with counter assigned is changed to a Layer 2 port or removed, the hardware
counters are freed. This action is similar to issuing the **no counter** command.

Examples This example shows how to assign a counter set to a switch port: Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#interface vlan 20 Switch(config-if)#counter Switch(config-if)#end Switch#

dbl

L

To enable active queue management on a transmit queue used by a class of traffic, use the **dbl** command. Use the **no** form of this command to return to the default setting.

dbl

no dbl

Syntax Description This command has no keywords or arguments	its.
--	------

Defaults	Active queue management is	disabled.
----------	----------------------------	-----------

Command Modes Policy-map class configuration

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	12.2(40)SG	Added support for the Supervisor Engine 6E.

Usage Guidelines The semantics of the DBL configuration is similar to (W)RED algorithm. That means 'dbl' is allowed standalone on "class-default", but otherwise requires that bandwidth or shape command also be configured on the class.

 Examples
 This example shows how to enable dbl action in a class:

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

 Switch(config)# policy-map policy1
 Switch(config-pmap)# class class1

 Switch(config-pmap-c)# dbl
 Switch(config-pmap-c)# exit

 Switch(config-pmap)# exit
 Switch(config-pmap)# exit

Switch(config-pmap-c)# dbl
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# end

Related Commands	Command	Description
	bandwidth	Creates a signaling class structure that can be referred to by its
		name.
	class	Creates a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration
		mode.

Command	Description
policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
service-policy (policy-map class)	Creates a service policy that is a quality of service (QoS) policy within a policy map.
show policy-map	Displays information about the policy map.

debug adjacency

To display information about the adjacency debugging, 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 (Opti	tional) Displays the IPC entries in the adjacency database.
Defaults	This command h	has no default settings.
Command Modes	Privileged EXE	C mode
Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	4d02h: ADJ: ad 4d02h: ADJ: ad 4d02h: ADJ: ad 4d02h: ADJ: ad 4d02h: ADJ: ad 4d02h: ADJ: ad	<pre>dd 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00 dd 172.20.52.36 (GigabitEtherne</pre>
Related Commands	Command	Description
	undebug adjac no debug adjace	

debug backup

To debug the backup events, use the **debug backup** command. To disable the 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 mode

 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 backup events:

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

Related Commands	Command	Description	
	undebug backup (same as no debug backup)	Disables debugging output.	

debug condition interface

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

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

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

Syntax Description	fastethernet	Limits the debugging to Fast Ethernet interfaces.	
	mod/port	Number of the module and port.	
	GigabitEthernet	Limits the debugging to Gigabit Ethernet interfaces.	
	null interface-num	Limits the debugging to null interfaces; the valid value is 0.	
	port-channel interface-	<i>num</i> Limits the debugging to port-channel interfaces; valid values are from 1 to 64.	
	vlan vlan_id	Specifies the VLAN interface number; valid values are from 1 to 4094.	
Defaults	This command has no de	fault settings.	
Command Modes	Privileged EXEC mode		
Command History	Release Modif	ication	
	12.1(8a)EW Suppo	ort for this command was introduced on the Catalyst 4500 series switch.	
	12.1(12c)EW Suppo	ort for extended VLAN addresses added.	
	This example shows how	shows how to limit the debugging output to VLAN interface 1:	
Examples	-		
Examples	Switch# debug conditic Condition 2 set Switch#		
	Switch# debug conditic Condition 2 set		
Examples Related Commands	Switch# debug conditic Condition 2 set Switch#	on interface vlan 1	

debug condition standby

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

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

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

Syntax Description	fastethernet	Limits the debugging to Fast Ethernet interfaces.
	mod/port	Number of the module and port.
	GigabitEthernet	Limits the debugging to Gigabit Ethernet interfaces.
	port-channel inte	<i>rface_num</i> Limits the debugging output to port-channel interfaces; valid values are from 1 to 64.
	vlan vlan_id	Limits the debugging of a condition on a VLAN interface; valid values are from 1 to 4094.
	group-number	VLAN group number; valid values are from 0 to 255.
Defaults	This command has	no default settings.
Command Modes	Privileged EXEC r	ıode
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 \mathbf{n} to abort the removal or \mathbf{y} to proceed with the removal. If you remove the only condition set, an excessive number of debugging messages might occur.	
	you remove the on	y condition set, an excessive number of debugging messages might occur.
Examples		y condition set, an excessive number of debugging messages might occur. as how to limit the debugging output to group 0 in VLAN 1:

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
are first removed.
Proceed with removal? [yes/no]: n
% Operation aborted
```

```
Switch#
```

Related Commands	Command	Description
	undebug condition standby (same as no debug condition standby)	Disables debugging output.

debug condition vlan

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

debug condition vlan {*vlan_id*}

no debug condition vlan {*vlan_id*}

	<i>vlan_id</i> Nu	umber of the VLAN; valid values are from 1 to 4096.	
Defaults	This command has no default settings. Privileged EXEC mode		
Command Modes			
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.	
	•	rt the removal operation. You can enter \mathbf{n} to abort the removal or \mathbf{y} to proceed with the remove the only condition set, it could result in the display of an excessive number of	
Examples	removal. If you messages.	remove the only condition set, it could result in the display of an excessive number of	
Examples	removal. If you messages. This example sh	remove the only condition set, it could result in the display of an excessive number of ows how to limit the debugging output to VLAN 1: condition vlan 1	
Examples	removal. If you messages. This example sh Switch# debug Condition 4 se Switch#	remove the only condition set, it could result in the display of an excessive number of ows how to limit the debugging output to VLAN 1: condition vlan 1	
Examples	removal. If you messages. This example sh Switch# debug Condition 4 se Switch# This example sh condition: Switch# no deb This condition Removing all c	remove the only condition set, it could result in the display of an excessive number of ows how to limit the debugging output to VLAN 1: condition vlan 1 t ows the message that is displayed when you attempt to disable the last VLAN debug ug condition vlan 1 is the last vlan condition set. onditions may cause a flood of debugging sult, unless specific debugging flags	

Related Commands	Command	Description
	undebug condition vlan (same as no debug condition vlan)	Disables debugging output.

debug dot1x

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

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

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

Syntax Description	all	Enables the debugging of all conditions.		
	errors	Enables the debugging of print statements guarded by the dot1x error flag.		
	events	Enables the debugging of print statements guarded by the dot1x events flag.		
	packets	All incoming dot1x packets are printed with packet and interface information.		
	registry	Enables the debugging of print statements guarded by the dot1x registry flag.		
	state-machine	Enables the debugging of print statements guarded by the dot1x registry flag.		
Defaults	Debugging is disabled	1.		
Command Modes	Privileged EXEC mode			
Command History	Release Mo	odification		
-	12.1(12c)EW Su	pport for this command was introduced on the Catalyst 4500 series switch.		
Examples	This example shows how to enable the 802.1X debugging for all conditions:			
	Switch# debug dot1x all Switch#			
Related Commands	Command	Description		
	show dot1x	Displays dot1x information.		
	undebug dot1x (sam debug dot1x)	e as no Disables debugging output.		
	•	e as no Disables debugging output.		
debug etherchnl

debug etherchnl

To debug EtherChannel, use the debug etherchnl command. To disable the 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 the detailed EtherChannel debug messages.				
	error	r (Optional) Displays the EtherChannel error messages.				
	event	(Optional) Debugs the major EtherChannel event messages.				
	idb	(Optional) Debugs the PAgP IDB messages.				
	linecard	(Optional) Debugs the SCP messages to the module.				
Defaults	The default set	tings are as follows:				
	• Debug is disabled.					
	-	ges are displayed.				
Command Modes	Privileged EXI	EC mode				
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 s	shows how to display all the EtherChannel debug messages:				
-	<pre>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#</pre>					
	This example shows how to display the EtherChannel IDB debug messages:					
	Switch# debug	Switch# debug etherchnl idb Agport idb related debugging is on Switch#				

This example shows how to disable the debugging:

Switch# **no debug etherchnl** Switch#

Command

Related Commands

Description

undebug etherchnl (same as no Disables debugging output. debug etherchnl)

debug interface

To abbreviate the 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 mod/port | **GigabitEthernet** mod/port | **null** | **port-channel** interface-num | **vlan** vlan_id}

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

Syntax Description	FastEthernet	Limits the debugging to Fast Ethernet interfaces.	
	mod/port	Number of the module and port.	
	GigabitEthernet	Limits the debugging to Gigabit Ethernet interfaces.	
	null	Limits the debugging to null interfaces; the only valid value is 0.	
	port-channel interface-num	 Limits the debugging to port-channel interfaces; valid values are from 1 to 64. 	
	vlan vlan_id	Specifies the VLAN interface number; valid values are from 1 to 4094.	
Defaults	This command has no defau	lt settings.	
Command Modes	Privileged EXEC mode		
Command History	Release Modifica	tion	
	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 the debugging to interface VLAN 1:	
	Switch# debug interface vlan 1 Condition 1 set Switch#		
Related Commands	Command	Description	
	debug condition interface	Limits the debugging output of interface-related activities.	
	undebug etherchnl (same a	s no Disables debugging output.	

debug ipc

To debug the IPC activity, use the **debug ipc** command. To disable the 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 the IPC error debugging.
	events	Enables the IPC event debugging.
	headers	Enables the IPC header debugging.
	packets	Enables the IPC packet debugging.
	ports	Enables the debugging of the creation and deletion of ports.
	seats	Enables the debugging of the creation and deletion of nodes.
Defaults	This command	has no default settings.
Command Modes	Privileged EXE	EC mode
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 the debugging of the IPC events: Switch# debug ipc events Special Events debugging is on Switch#	
Related Commands	Command undebug ipc (s ipc)	Description same as no debug Disables debugging output.

debug ip dhcp snooping event

To debug the 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 mode

 Release
 Modification

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

ExamplesThis example shows how to enable the debugging for the DHCP snooping events:
Switch# debug ip dhcp snooping event
Switch#This example shows how to disable the debugging for the DHCP snooping events:
Switch# no debug ip dhcp snooping event
Switch#

Related Commands	Command	Description
	debug ip dhcp snooping packet	Debugs the DHCP snooping messages.

debug ip dhcp snooping packet

To debug the DHCP snooping messages, use the **debug ip dhcp snooping packet** command. To disable the 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 mode

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 the debugging for the DHCP snooping packets: Switch# debug ip dhcp snooping packet Switch# This example shows how to disable the debugging for the DHCP snooping packets: Switch# no debug ip dhcp snooping packet Switch# Switch#

Related Commands	Command	Description
	debug ip dhcp snooping event	Debugs the DHCP snooping events.

debug ip verify source packet

To debug the IP source guard messages, use the **debug ip verify source packet** command. To disable the 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 mode

 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 the IP source guard: Switch# debug ip verify source packet Switch#

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

Switch# no debug ip verify source packet Switch#

Related Commands	Command	Description
	ip dhcp snooping	Globally enables DHCP snooping.
	ip dhcp snooping limit rate	Enables DHCP option 82 data insertion.
	ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
	show ip dhcp snooping	Displays the DHCP snooping configuration.
	show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

debug lacp

To debug the LACP activity, use the **debug lacp** command. To disable the 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 the debugging of the LACP events.
	fsm	(Optional) Enables the debugging of the LACP finite state machine.
	misc	(Optional) Enables the miscellaneous LACP debugging.
	packet	(Optional) Enables the LACP packet debugging.
Defaults	Debugging of L	ACP activity is disabled.
Command Modes	Privileged EXE	C mode
Command History	Release	Modification
Command History	Release 12.1(13)EW	ModificationSupport for this command was introduced on the Catalyst 4500 series switch.
	12.1(13)EW This command	
Usage Guidelines	12.1(13)EW This command in Catalyst 4500 se	Support for this command was introduced on the Catalyst 4500 series switch.
Command History Usage Guidelines Examples	12.1(13)EW This command in Catalyst 4500 so This example sh Switch# debug	Support for this command was introduced on the Catalyst 4500 series switch. is supported only by the supervisor engine and can be entered only from the eries switch console.
Usage Guidelines	12.1(13)EW This command in Catalyst 4500 so This example sh Switch# debug Port Aggregati	Support for this command was introduced on the Catalyst 4500 series switch. is supported only by the supervisor engine and can be entered only from the eries switch console.

debug monitor

To display the monitoring activity, use the **debug monitor** command. To disable the 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 the SPAN debugging messages.	
	errors	Displays the SPAN error details.	
	idb-update	Displays the SPAN IDB update traces.	
	list	Displays the SPAN list tracing and the VLAN list tracing.	
	notifications	Displays the SPAN notifications.	
	platform	Displays the SPAN platform tracing.	
	requests	Displays the SPAN requests.	
Defaults	This command l	nas no default settings.	
Command Modes	Privileged EXE	C mode	
Command History	Release	Modification	
Command History	Release 12.1(8a)EW		
	12.1(8a)EW	Modification	•
Command History Examples	12.1(8a)EW This example sh Switch# debug	Modification Support for this command was introduced on the Catalyst 4500 series switch	
	12.1(8a)EW This example sh Switch# debug SPAN error det	Modification Support for this command was introduced on the Catalyst 4500 series switch nows how to debug the monitoring errors: monitor errors	

debug nvram

To debug the NVRAM activity, use the **debug nvram** command. To disable the 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 mode

 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	Command	Description
	undebug nvram (same as no debug nvram)	Disables debugging output.

debug pagp

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

debug pagp [all | dual-active | event | fsm | misc | packet]

no debug pagp

yntax Description	all	(Optional) Enables all PAgP debugging.	
	dual-active	(Optional) Enables the PAgP dual-active debugging.	
	event	(Optional) Enables the debugging of the PAgP events.	
	fsm	(Optional) Enables the debugging of the PAgP finite state machine.	
	misc	(Optional) Enables the miscellaneous PAgP debugging.	
	packet	(Optional) Enables the PAgP packet debugging.	
Defaults	This command	has no default settings.	
Command Modes	Privileged EXE	C mode	
Command History	Release	Modification	
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.	
Jsage Guidelines	This command is supported only by the supervisor engine and can be entered only from the Catalyst 4500 series switch console.		
Examples	This example sl	hows how to enable the PAgP miscellaneous debugging:	
		pagp misc ion Protocol Miscellaneous debugging is on	
	*Sep 30 10:13 *Sep 30 10:13	:03: SP: PAgP: pagp_h(Fa5/6) expired :03: SP: PAgP: 135 bytes out Fa5/6 :03: SP: PAgP: Fa5/6 Transmitting information packet :03: SP: PAgP: timer pagp_h(Fa5/6) started with interval 30000 cuncated>	
Related Commands	*Sep 30 10:13 *Sep 30 10:13 *Sep 30 10:13 *Sep 30 10:13 *Sep 30 10:13	:03: SP: PAgP: 135 bytes out Fa5/6 :03: SP: PAgP: Fa5/6 Transmitting information packet :03: SP: PAgP: timer pagp_h(Fa5/6) started with interval 30000	

2-85

debug platform packet protocol lacp

To debug the LACP protocol packets, use the **debug platform packet protocol lacp** command. To disable the 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 the	platform packet reception debugging functions.
	transmit	(Optional) Enables the	platform packet transmission debugging functions.
	vlan	(Optional) Enables the	platform packet VLAN debugging functions.
Defaults	This command l	has no default settings.	
command Modes	Privileged EXE	C mode	
Command History	Release	Modification	
	12.1(8a)EW	Support for this comma	and was introduced on the Catalyst 4500 series switch.
Examples	This example sh	nows how to enable all PM	debugging:
	Switch# debug Switch#	platform packet protoco	ol lacp
Related Commands	Command		Description
		orm packet protocol lacp	Disables debugging output.

debug platform packet protocol pagp

To debug the PAgP protocol packets, use the **debug platform packet protocol pagp** command. To disable the 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	(Optional) Enables the	platform packet reception debugging functions.
	transmit	(Optional) Enables the	platform packet transmission debugging functions.
	vlan	(Optional) Enables the	platform packet VLAN debugging functions.
Defaults	This command	has no default settings.	
Command Modes	Privileged EXE	C mode	
Command History	Release	Modification	
	12.1(13)EW	Support for this comma	and was introduced on the Catalyst 4500 series switch.
Examples	This example sh	nows how to enable all PM	debugging:
	Switch# debug Switch#	platform packet protoco	bl pagp
Related Commands	Command		Description
	• •	orm packet protocol no debug platform packet	Disables debugging output.

debug pm

To debug the port manager (PM) activity, use the **debug pm** command. To disable the 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}

card Debugs the module-related events. cookies Enables the internal PM cookie validation. etherchnl Debugs the EtherChannel-related events. messages Debugs the PM messages. port Debugs the PM registry invocations. scp Debugs the SCP module messaging. sm Debugs the state machine-related events. span Debugs the state machine-related events. split Debugs the spanning-tree-related events. split Debugs the virtual port-related events. vian Debugs the virtual port-related events. vp Debugs the virtual port-related events.	Syntax Description	all	Displays all PM debugg	ing messages.		
etherchnl Debugs the EtherChannel-related events. messages Debugs the PM messages. port Debugs the port-related events. registry Debugs the PM registry invocations. scp Debugs the SCP module messaging. sm Debugs the state machine-related events. span Debugs the spaning-tree-related events. split Debugs the split-processor. vlan Debugs the virtual port-related events. vp Debugs the virtual port-related events. vs Privileged EXEC mode 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# Geomand	-	card				
messages Debugs the PM messages. port Debugs the port-related events. registry Debugs the SCP module messaging. scp Debugs the SCP module messaging. sm Debugs the state machine-related events. span Debugs the split-processor. vlan Debugs the VLAN-related events. vp Debugs the virtual port-related events. Virtual port-related events Virtual port-related events. Virtual port-re		cookies	Enables the internal PM	cookie validation.		
port Debugs the port-related events. registry Debugs the PM registry invocations. scp Debugs the SCP module messaging. sm Debugs the state machine-related events. span Debugs the split-processor. vlan Debugs the VLAN-related events. yp Debugs the virtual port-related events. vp Debugs the virtual port-related events. Privileged EXEC mode Privileged EXEC mode 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 Command Description		etherchnl	Debugs the EtherChann	el-related events.		
registry Debugs the PM registry invocations. scp Debugs the SCP module messaging. sm Debugs the state machine-related events. span Debugs the spanning-tree-related events. split Debugs the split-processor. vlan Debugs the VLAN-related events. vp Debugs the virtual port-related events. Vanter This command has no default settings. Command Modes Privileged EXEC mode Examples Modification 12.1(8a)EW Support for this command was introduced on the Catalyst 4500 series switch. Switch# debug pm all Switch# debug pm all Switch# Descriptio		messages Debugs the PM messages.				
scp Debugs the SCP module messaging. sm Debugs the state machine-related events. span Debugs the spanning-tree-related events. split Debugs the split-processor. vlan Debugs the VLAN-related events. vp Debugs the virtual port-related events. Value This command has no default settings. Command Modes Privileged EXEC mode Examples Modification 12.1(8a)EW Support for this command was introduced on the Catalyst 4500 series switch. Switch# Gebug pm all Switch# Gebug pm all Switch# Description		port Debugs the port-related events.				
sm Debugs the state machine-related events. span Debugs the spanning-tree-related events. split Debugs the split-processor. vlan Debugs the VLAN-related events. vp Debugs the virtual port-related events. vp Debugs the virtual port-related events. Privileged EXEC mode Privileged EXEC mode 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# debug pm all Related Commands Command		registry	Debugs the PM registry	invocations.		
span Debugs the spanning-tree-related events. split Debugs the split-processor. vlan Debugs the VLAN-related events. vp Debugs the virtual port-related events. pefaults This command has no default settings. Command Modes Privileged EXEC mode 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# Description		scp	Debugs the SCP module	e messaging.		
split Debugs the split-processor. vlan Debugs the VLAN-related events. vp Debugs the virtual port-related events. Defaults This command has no default settings. Command Modes Privileged EXEC mode 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# Description		sm	Debugs the state machin	ne-related events.		
vlan Debugs the VLAN-related events. vp Debugs the virtual port-related events. Defaults This command has no default settings. Command Modes Privileged EXEC mode 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# Description		span	Debugs the spanning-tre	ee-related events.		
vp Debugs the virtual port-related events. Defaults This command has no default settings. Command Modes Privileged EXEC mode 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 Related Commands Command Description		split	Debugs the split-proces	sor.		
Defaults This command has no default settings. Command Modes Privileged EXEC mode 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# Description		vlan	Debugs the VLAN-relat	red events.		
Command Modes Privileged EXEC mode 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# Description		vp	Debugs the virtual port-	related events.		
Examples This example shows how to enable all PM debugging: Switch# debug pm all Switch# Related Commands Command Description						
Examples This example shows how to enable all PM debugging: Switch# debug pm all Switch# Related Commands Command Description	-	12.1(8a)EW	Support for this comma	nd was introduced on the Catalyst 4500 series switch.		
	Examples	Switch# debug		debugging:		
undebug pm (same as no debug pm) Disables debugging output.	Related Commands	Command		Description		
		undebug pm (same as no debug pm)	Disables debugging output.		

debug port-security

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

debug port-security

no debug port-security

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

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 Catalyst 4500 series switch.

Examples This example shows how to enable all PM debugging: Switch# debug port-security Switch#

Related Commands	Command	Description
	switchport port-security	Enables port security on an interface.

debug redundancy

To debug the supervisor engine redundancy, use the **debug redundancy** command. To disable the 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 the redundancy facility for error debugging.	
	fsm	Enables the redundancy facility for FSM event debugging.	
	kpa	Enables the redundancy facility for keepalive debugging.	
	msg	Enables the redundancy facility for messaging event debugging.	
	progression	Enables the redundancy facility for progression event debugging.	
	status	Enables the redundancy facility for status event debugging.	
	timer	Enables the redundancy facility for timer event debugging.	
Command Modes	Privileged EXE		
Command History	Release	Modification	
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch (Catalyst 4507R only).	
Examples	-	hows how to debug the redundancy facility timer event debugging: redundancy timer	

debug spanning-tree

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

debug spanning-tree {all | backbonefast | bpdu | bpdu-opt | etherchannel | config | events | exceptions | general | ha | mstp | pvst+ | root | snmp | switch | synchronization | uplinkfast}

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

	<u> </u>			
Syntax Description	all	Displays all the spanning-tree debugging messages.		
	backbonefast	Debugs the backbonefast events.		
	bpdu	Debugs the spanning-tree BPDU.		
	bpdu-opt	Debugs the optimized BPDU handling.		
	etherchannel	el Debugs the spanning-tree EtherChannel support.		
	config	Debugs the spanning-tree configuration changes.		
	events	Debugs the TCAM events.		
	exceptions	Debugs the spanning-tree exceptions.		
	general	Debugs the general spanning-tree activity.		
	ha	Debugs the HA events		
	mstp	Debugs the multiple spanning-tree events.		
	pvst+	Debugs the PVST+ events.		
	root	Debugs the spanning-tree root events.		
	snmp	Debugs the spanning-tree SNMP events.		
	switch	Debugs the switch debug events.		
	synchronization	Debugs the STP state synchronization events.		
	uplinkfast Debugs the uplinkfast events.			
Defaults Command Modes	This command has Privileged EXEC	s no default settings. mode		
Command History	Release	Modification		
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.		
Examples	This example show	vs how to debug the spanning-tree PVST+:		

Related Commands	Command	Description	
	undebug spanning-tree (same as no	Disables debugging output.	
	debug spanning-tree)		

2-93

debug spanning-tree backbonefast

To enable debugging of the spanning-tree BackboneFast events, use the **debug spanning-tree backbonefast** command. To disable the 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 the	e detailed BackboneFast debugging messages.
	exceptions	(Optional) Enables the	debugging of spanning-tree BackboneFast exceptions.
Defaults	This command	has no default settings.	
Command Modes	Privileged EXE	C mode	
Command History	Release	Modification	
	12.1(8a)EW	Support for this comm	and was introduced on the Catalyst 4500 series switch.
Examples	Catalyst 4500 series switch console. This example shows how to enable the debugging and to display the detailed spanning-tree		
	BackboneFast debugging information: Switch# debug spanning-tree backbonefast detail Spanning Tree backbonefast detail debugging is on Switch#		
Related Commands	Command		Description
		ning-tree backbonefast bug spanning-tree	Disables debugging output.

debug spanning-tree switch

To enable the switch shim debugging, use the **debug spanning-tree switch** command. To disable the 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 the spanning-tree switch shim debugging messages.		
	errorsEnables the debugging of switch shim errors or exceptions.generalEnables the debugging of general events.		
	pm	Enables the debugging of port manager events.	
	rx	Displays the received BPDU-handling debugging messages.	
	decode	Enables the debugging of the decode-received packets of the spanning-tree switch shim.	
	errors	Enables the debugging of the receive errors of the spanning-tree switch shim.	
	interrupt	Enables the shim ISR receive BPDU debugging on the spanning-tree switch.	
	process	Enables the process receive BPDU debugging on the spanning-tree switch.	
	state	te Enables the debugging of the state changes on the spanning-tree port.	
	tx	Enables the transmit BPDU debugging on the spanning-tree switch shim.	
	decode (Optional) Enables the decode-transmitted packets debugging on the spanning-tree switch shim.		
Defaults	This command	has no default settings.	
Command Modes	Privileged EXI	EC mode	
Command History	Release	Modification	
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.	
Usage Guidelines	This command console.	is supported only by the supervisor engine and can be entered only from the switch	

Examples	This example shows how to enable the 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	Command Description						
	undebug spanning-tree switch (same as Disables debugging output. no debug spanning-tree switch)						

debug spanning-tree uplinkfast

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

debug spanning-tree uplinkfast [exceptions]

no debug spanning-tree uplinkfast

Syntax Description	exceptions	(Optional) Enables the debugging of the spanning-tree UplinkFast exceptions.	
Defaults	This command l	nas no default settings.	
Command Modes	Privileged EXEC mode		
Command History	Release 12.1(8a)EW	Modification Support for this command was introduced on the Catalyst 4500 series switch.	
Usage Guidelines	This command i console.	s supported only by the supervisor engine and can be entered only from the switch	
Examples	This example shows how to debug the spanning-tree UplinkFast exceptions: Switch# debug spanning-tree uplinkfast exceptions Spanning Tree uplinkfast exceptions debugging is on Switch#		
Related Commands	~ .	Description ing-tree uplinkfast Disables debugging output. bug spanning-tree Disables debugging output.	

debug sw-vlan

To debug the VLAN manager activities, use the **debug sw-vlan** command. To disable the 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 the VLAN	manager incidents of bad port-manager cookies.	
	events	Debugs the VLAN r	nanager events.	
	management	managementDebugs the VLAN manager management of internal VLANs.		
	packets Debugs the packet handling and encapsulation processes.		andling and encapsulation processes.	
	registries	Debugs the VLAN r	nanager registries.	
Defaults	This command ha	as no default settings.		
Command Modes	Privileged EXEC	mode		
Command History	Release	Modification		
	12.1(8a)EW	Support for this comm	hand was introduced on the Catalyst 4500 series switch.	
Examples	This example sho	ws how to debug the so	ftware VLAN events:	
	Switch# debug s vlan manager ev Switch#	w-vlan events ents debugging is on		
Related Commands	Command		Description	

debug sw-vlan ifs

To enable the VLAN manager Cisco IOS file system (IFS) error tests, use the **debug sw-vlan ifs** command. To disable the 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	open	Enables the VLAN manager IFS debugging of errors in an IFS file-open operation.		
	read Debugs the errors that occurred when the IFS VLAN configuration file was reading.			
	write Debugs the errors that occurred when the IFS VLAN configuration file was writing.			
	$\{1 \mid 2 \mid 3 \mid 4\}$	Determines the file-read operation. See the "Usage Guidelines" section for information about operation levels.		
	write	Debugs the errors that occurred during an IFS file-write operation.		
Defaults	This command	has no default settings.		
Command Modes	Privileged EXE	C mode		
Command History	Release Modification			
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.		
Usage Guidelines	The following a	are four types of file read operations:		
	• Operation 2 number.	1—Reads the file header, which contains the header verification word and the file version		
	• Operation 2 information	2—Reads the main body of the file, which contains most of the domain and VLAN n.		
	• Operation 3 —Reads TLV descriptor structures.			
	• Operation 4—Reads TLV data.			
Examples	This example s	hows how to debug the TLV data errors during a file-read operation:		
	-	<pre>sw-vlan ifs read 4 ifs read # 4 errors debugging is on</pre>		

Related Commands	Command	Description	
	undebug sw-vlan ifs (same as no debug sw-vlan ifs)	Disables debugging output.	

debug sw-vlan notification

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

debug sw-vlan notification {accfwdchange | allowedvlancfgchange | fwdchange | linkchange | modechange | pruningcfgchange | statechange}

no debug sw-vlan notification {accfwdchange | allowedvlancfgchange | fwdchange | linkchange | modechange | pruningcfgchange | statechange}

Syntax Description	-		the VLAN manager notification of aggregated access interface vard changes.	
	allowedvlancfgc	-	Enables the VLAN manager notification of changes to allowed VLAN configuration.	
	fwdchange	Enables the	e VLAN manager notification of STP forwarding changes.	
	linkchange	Enables the	e VLAN manager notification of interface link state changes.	
	modechange	Enables the	e VLAN manager notification of interface mode changes.	
	pruningcfgchan	-	Enables the VLAN manager notification of changes to pruning configuration.	
	statechange	Enables the	e VLAN manager notification of interface state changes.	
Defaults Command Modes	This command ha	as no default settings. mode		
Command History	Release	Modification		
	12.1(8a)EW	Support for this comm		
		Support for this comma	and was introduced on the Catalyst 4500 series switch.	
Examples			and was introduced on the Catalyst 4500 series switch. tware VLAN interface mode change notifications:	
Examples	This example sho	ws how to debug the sof	tware VLAN interface mode change notifications:	
Examples Related Commands	This example sho Switch# debug s vlan manager po	ws how to debug the sof	tware VLAN interface mode change notifications:	

debug sw-vlan vtp

To enable the debugging of messages to be generated by the VTP protocol code, use the **debug sw-vlan vtp** command. To disable the 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	events Displays the 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 Cisco IOS VTP platform-dependent layer, except for pruning packets.		
	pruning Enables the debugging message to be generated by the pruning segment of the VT protocol code.			
	packets(Optional) Displays the contents of all incoming VTP pruning packets that have passed into the VTP code from the Cisco IOS VTP platform-dependent layer.			
	xmit	(Optional) Displays the contents of all outgoing VTP packets that the VTP code will request that the Cisco IOS VTP platform-dependent layer to send.		
	xmit	Displays the contents of all outgoing VTP packets that the VTP code will request that the Cisco IOS VTP platform-dependent layer to send; does not include pruning packets		
Defaults	This comma	nd has no default settings.		
Command Modes	Privileged E	KEC mode		
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 exampl	shows how to debug the software VLAN outgoing VTP packets:		
		ng sw-vlan vtp xmit Dugging is on		
Related Commands	Command	Description		

debug udld

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

debug udld {events | packets | registries}

no debug udld {events | packets | registries}

Syntax Description	events	Enables the debugging of UDLD process events as they occur.		
	packets Enables the debugging of the UDLD process as it receives packets from the packet qu			
	and attempts to transmit packets at the request of the UDLD protocol code.			
	registries	Enables the debugging of the UDLD process as it processes registry upcalls from the		
		UDLD process-dependent module and other feature modules.		
Defaults	This command	d has no default settings.		
Command Modes	Privileged EX	EC mode		
Command History	Release	Modification		
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.		
-		d is supported only by the supervisor engine and can be entered only from the series switch console.		
Examples	This example	shows how to debug the UDLD events:		
		g udld events debugging is on		
	This example shows how to debug the UDLD packets:			
	Switch# debug udld packets UDLD packets debugging is on Switch#			
	This example	shows how to debug the UDLD registry events:		
		g udld registries ies debugging is on		

Related Commands	Command	Description
	undebug udld (same as no debug udld)	Disables debugging output.

debug vqpc

To debug the VLAN Query Protocol (VQP), use the **debug vqpc** command. To disable the 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	the VOP events		
oymax booonprion	cli (Optional) Debugs the VQP command-line interface.				
		events (Optional) Debugs the VQP events.			
	learn				
	packet	(Optional) Debugs the	v VQP packets.		
Defaults	This command	has no default settings.			
Command Modes	Privileged EXEC mode				
Command History	Release	Modification			
	12.1(13)EW	Support for this comm	nand was introduced on the Catalyst 4500 series switch.		
Examples	This example sł	nows how to enable all V	QP debugging:		
	Switch# debug vqpc all Switch#				
Related Commands	Command		Description		
	vmps reconfirm	m (privileged EXEC)	Immediately sends VLAN Query Protocol (VQP) queries to reconfirm all the dynamic VLAN assignments with the VLAN Membership Policy Server (VMPS).		

define interface-range

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

define interface-range macro-name interface-range

Syntax Description	macro-name	Name of the interface range macro; up to 32 characters.			
oyntax bescription	interface-range	List of valid ranges when specifying interfaces; see the "Usage Guidelines" section.			
Defaults	This command has no default settings.				
Command Modes	Global configuration mode				
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 <i>interface-range</i>, use these formats: <i>interface-type</i> {mod}/{first-interface} - {last-interface} 				
	 interface-type {mod}/{first-interface} - {last-interface} 				
	The valid values for <i>interface-type</i> are as follows:				
	FastEthernet GigsbitEthernet				
	 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	Command	Description			
	interface range	Runs a command on multiple ports at the same time.			

deny

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

- 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.
	ір	Specifies the sender IP address.
	any	Specifies that any IP or MAC address will be accepted.
	host sender-ip	Specifies that only a specific sender IP address will be accepted.
	sender-ip sender-ip-mask	Specifies that a specific range of sender IP addresses will be accepted.
	mac	Specifies the sender MAC address.
	host sender-mac	Specifies that only a specific sender MAC address will be accepted.
	sender-mac sender-mac-mask	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 target-ip	(Optional) Specifies that only a specific target IP address will be accepted.
	target-ip target-ip-mask	(Optional) Specifies that a specific range of target IP addresses will be accepted.
	mac	Specifies the MAC address values for the ARP responses.
	host target-mac	(Optional) Specifies that only a specific target MAC address will be accepted.
	target-mac target-mac-mask	(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 b	added to forward or drop ARP packets based on some matching criteria.			
Examples	This example shows a host with a MAC address of 0000.0000.abcd and an IP address of 1.1.1.1. This example shows howto deny both requests and responses from this host:				
	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 s deny ip host Switch#	atic-hosts .1.1.1 mac host 0000.0000.abcd			
Related Commands	Command	Description			
	arp access-list	Defines an ARP access list or adds clauses at the end of a predefined list.			
	ip arp inspection	Ilter vlan Permits ARPs from hosts that are configured for static IP when DAI is enabled and to define an ARP access list and applies it to a VLAN.			
	permit	Permits an ARP packet based on matches against the DHCP bindings.			

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	and remov) Specifies that the bootup SRAM diagnostics log all failures ye all affected buffers from the hardware operation. The RAM diagnostics will log events, but will take no other
	normal	conservati	Specifies that the SRAM diagnostics operate as in ve mode, except that an ongoing failure resets the supervisor lows for the bootup tests to map out the affected memory.
	aggressive	mode, exc the superv	Specifies that the SRAM diagnostics operate as in normal ept that a bootup failure only logs failures and does not allow risor engine to come online; allows for either a redundant rengine or network-level redundancy to take over.
Defaults	normal mode		
Command Modes	Global configuration mode		
Command History	Release M	lodification	
	12.2(18)EW T	his 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 redundancy has been provid	•	we redundant supervisor engines, or when network-level
Examples	This example shows how to configure the switch to initiate an RPR switchover when an ongoing failure occurs:		
	Switch# configure termin Switch (config)# diagnos		action normal
Related Commands	Command		Description
	show diagnostic result mo	dule test 2	Displays the module-based diagnostic test results.
	show diagnostic result mo	dule test 3	Displays the module-based diagnostic test results.
			-

diagnostic start

To run the specified diagnostic test, use the diagnostic start command.

diagnostic start {module num} {test test-id} [port num]

Syntax Description	module num	Module number.	
	test	Specifies a test to run.	
	test-id	Specifies an identification number for the test to be run; can be the cable diagnostic <i>test-id</i> , or the cable-tdr keyword.	
	port num	(Optional) Specifies the interface port number.	
Defaults	This command	has no default settings.	
Command Modes	Privileged EXE	C mode	
Command History	Release	Modification	
	12.2(25)SG	Support for this command was introduced on the Catalyst 4500 series switch.	
Examples	This example shows how to run the specified diagnostic test at the specified module: This exec command starts the TDR test on specified interface Switch# diagnostic start module 1 test cable-tdr port 3 diagnostic start module 1 test cable-tdr port 3 module 1: Running test(s) 5 Run interface level cable diags module 1: Running test(s) 5 may disrupt normal system operation Do you want to continue? [no]: yes yes Switch# 2d16h: %DIAG-6-TEST_RUNNING: module 1: Running online-diag-tdr{ID=5} 2d16h: %DIAG-6-TEST_OK: module 1: online-diag-tdr{ID=5} has completed successfully Switch#		
Note	The show cable-diagnostic tdr command is used to display the results of a TDR test. The test results will not be available until approximately 1 minute after the test starts. If you type the show cable-diagnostic tdr command within 1 minute of the test starting, you may see a "TDR test is in progress on interface" message.		
Related Commands	Command	Description	

dot1x auth-fail max-attempts

To configure the max number of attempts before a port is moved to the auth-fail VLAN, use the **dot1x auth-fail max-attempts** command. To return to the default setting, use the **no** form of this command.

dot1x auth-fail max-attempts max-attempts

no dot1x auth-fail max-attempts max-attempts

Syntax Description	<i>max-attempts</i> Specifies a maximum number of attempts before a port is moved to the				
		auth-fail VLAN in the range of 1 to 10.			
Defaults	Default is 3.				
Command Modes	Interface configu	ration mode			
Command History	Release	Modification			
	12.2(25)SG	Support for this command was introduced on the Catalyst 4500 series switch.			
Examples	This example shows how to configure the maximum number of attempts before the port is moved to the auth-fail VLAN on Fast Ethernet interface 4/3:				
	Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z.				
	Switch(config)# interface fastethernet4/3 Switch(config-if)# dot1x auth-fail max-attempts 5				
	Switch(config-i Switch#				
Related Commands	Command	Description			
	dot1x max-reau	th-req Sets the maximum number of times that the switch will retransmit an EAP-Request/Identity frame to the client before restarting the authentication process.			
	show dot1x	Displays dot1x information.			
dot1x auth-fail vlan

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

dot1x auth-fail vlan vlan-id

no dot1x auth-fail vlan vlan-id

Syntax Description	vlan-id	Specifies a VLAN in the range of 1 to 4094.	
Defaults	None		
Command Modes	Interface config	uration mode	
Command History	Release	Modification	
	12.2(25)SG	Support for this command was introduced on the Catalyst 4500 series switch.	
Examples	This example shows how to configure the auth-fail VLAN on Fast Ethernet interface 4/3: Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# interface fastethernet4/3 Switch(config-if)# dot1x auth-fail vlan 40 Switch(config-if)# end Switch#		
Related Commands	Command	Description	
	dot1x max-rea		
	show dot1x	Displays dot1x information.	

dot1x control-direction

To enable unidirectional port control on a per-port basis on a switch, use the **dot1x control-direction** command. Use the **no** form of this command to disable unidirectional port control.

dot1x control-direction [in | both]

no dot1x control-direction

Syntax Description	in	(Optional) Specifies controlling in-bound traffic on a port.	
	both	(Optional) Specifies controlling both in-bound and out-bound traffic on a port.	
Defaults	Both in-bound a	and out-bound traffic will be controlled.	
Command Modes	Interface configuration mode		
Command History	Release	Modification	
	12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switch.	
Usage Guidelines	You can manage remote systems using unidirectional control. Unidirectional control enables you to turn on systems remotely using a specific Ethernet packet, known as a magic packet. Using unidirectional control enables you to remotely manage systems using 802.1X ports. In the past, the port became unauthorized after the systems was turned off. In this state, the port only allowed the receipt and transmission of EAPoL packets. Therefore, there was no way for the unidirectional control magic packet to reach the host and without being turned on there was no way for the system to authenticate and open the port.		
Examples	-	hows how to enable unidirectional control on incoming packets: -if)# dot1x control-direction in -if)#	
Related Commands	Command	Description	
	show dot1x	Displays dot1x information.	

dot1x critical

To enable the 802.1X critical authentication on a port, use the **dot1x critical** command. To return to the default setting, use the **no** form of this command.

dot1x critical

no dot1x critical

Syntax Description	This command has no keywords or variables.
--------------------	--

Defaults	Critical authentication is disabled.
----------	--------------------------------------

Command Modes Interface configuration mode

 Command History
 Release
 Modification

 12.2(31)SG
 Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to enable 802.1x critical authentication:

Switch(config-if)# dot1x critical
Switch(config-if)#

Related Commands	Command	Description
	dot1x critical eapol	Enables sending EAPOL success packets when a port is critically authorized partway through an EAP exchange.
	dot1x critical recovery delay	Sets the time interval between port reinitializations.
	dot1x critical vlan	Assigns a critically authenticated port to a specific VLAN.
	show dot1x	Displays dot1x information.

dot1x critical eapol

To enable sending EAPOL success packets when a port is critically authorized partway through an EAP exchange, use the **dot1x critical eapol** command. To return to the default setting, use the **no** form of this command.

dot1x critical eapol

no dot1x critical eapol

Syntax Description	This command has no ke	eywords or variables.
--------------------	------------------------	-----------------------

- **Defaults** The default is to not send EAPOL success packets.
- **Command Modes** Global configuration mode

Command History	Release	Modification	
12.2(31)SG Support		Support for this command was introduced on the Catalyst 4500 series switch.	

Examples This example shows how to enable sending EAPOL success packets:

Switch(config-if)# dot1x critical eapol
Switch(config-if)#

Related Commands	Command	Description
	dot1x critical	Enables the 802.1X critical authentication on a port.
	dot1x critical recovery delay	Sets the time interval between port reinitializations.
	dot1x critical vlan	Assigns a critically authenticated port to a specific VLAN.
	show dot1x	Displays dot1x information.

dot1x critical recovery delay

To set the time interval between port reinitializations, use the **dot1x critical recovery delay** command. To return to the default setting, use the **no** form of this command.

dot1x critical recovery delay delay-time

no dot1x critical recovery delay

Syntax Description	delay-time	Specifies the interval between port reinitializations when AAA transistion occurs; valid values are from 1 to 10,000 milliseconds.			
Defaults	Delay time is set to 100 milliseconds.				
Command Modes	Global configurat	ion mode			
Command History	Release	Modification			
	12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switch.			
Examples	This example shows how to set the 802.1x critical recovery delay time to 500:				
	Switch(config-if Switch(config-if	f)# dot1x critical recovery delay 500 f)#			
Related Commands	Command	Description			
	dot1x critical	Enables the 802.1X critical authentication on a port.			
	dot1x critical ea	polEnables sending EAPOL success packets when a port is critically authorized partway through an EAP exchange.			
	dot1x critical vla	Assigns a critically authenticated port to a specific VLAN.			

dot1x critical vlan

To assign a critically authenticated port to a specific VLAN, use the **dot1x critical vlan** command. To return to the default setting, use the **no** form of this command

dot1x critical vlan vlan-id

no dot1x critical vlan-id

Syntax Description	vlan-id	(Optional)) Specifies the VLANs; valid values are from 1 to 4094.		
Defaults	Critical authentication is disabled on a ports VLAN.				
Command Modes	Interface config	guration mode			
Command History	Release	Modification			
	12.2(31)SG	Support for this c	command was introduced on the Catalyst 4500 series switch.		
Usage Guidelines	The type of VLAN specified must match the type of the port. If the port is an access port, the VLAN must be a regular VLAN. If the port is a private-VLAN host port, the VLAN must be the secondary VLAN of a valid private-VLAN domain. If the port is a routed port, no VLAN may be specified.				
	This command is not supported on platforms such as Layer 3 switches that do not include the Auth VLAN subsystem.				
Examples	This example s	hows how to enable 8	302.1x critical authentication on a ports VLAN:		
	Switch(config Switch(config	-if)# dot1x critica -if)#	al vlan 350		
Related Commands	Command		Description		
	dot1x critical		Enables the 802.1X critical authentication on a port.		
	dot1x critical	eapol	Enables sending EAPOL success packets when a port is critically authorized partway through an EAP exchange.		
	dot1x critical	recovery delay	Sets the time interval between port reinitializations.		
	show dot1x		Displays dot1x information.		

dot1x guest-vlan

dot1x guest-vlan

To enable a 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	vlan-id	Specifies a VLAN in the range of 1 to 4094.			
•)					
Defaults	None; the guest VLAN feature is disabled.				
Command Modes	Interface configuration mode				
Command History	Release	Modification			
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.			
	12.2(25)EWA	Support for secondary VLAN as the configured guest VLAN ID was added.			
Usage Guidelines	VLAN host ports	n be configured only on ports that are statically configured as access ports or private . Statically configured access ports can be configured with regular VLANs as guest v configured private VLAN host ports can be configured with secondary private			
	VLAN host ports	Statically configured access ports can be configured with regular VLANs as guest y configured private VLAN host ports can be configured with secondary private			
	VLAN host ports VLANs; statically VLANs as guest	. Statically configured access ports can be configured with regular VLANs as guest y configured private VLAN host ports can be configured with secondary private VLANs.			
Examples	VLAN host ports VLANs; statically VLANs as guest This example sho	. Statically configured access ports can be configured with regular VLANs as guest y configured private VLAN host ports can be configured with secondary private VLANs.			
	VLAN host ports VLANs; statically VLANs as guest This example sho Switch# configu	. Statically configured access ports can be configured with regular VLANs as guest y configured private VLAN host ports can be configured with secondary private VLANs.			
	VLAN host ports VLANs; statically VLANs as guest This example sho Switch# configura Switch(config)#	. Statically configured access ports can be configured with regular VLANs as guest y configured private VLAN host ports can be configured with secondary private VLANs. www. how to enable a guest VLAN on Fast Ethernet interface 4/3: re terminal tion commands, one per line. End with CNTL/Z. interface fastethernet4/3			
	VLAN host ports VLANs; statically VLANs as guest This example sho Switch# configura Switch(config)# Switch(config-i	 Statically configured access ports can be configured with regular VLANs as guest y configured private VLAN host ports can be configured with secondary private VLANs. bws how to enable a guest VLAN on Fast Ethernet interface 4/3: re terminal tion commands, one per line. End with CNTL/Z. 			
	VLAN host ports VLANs; statically VLANs as guest This example sho Switch# configura Switch(config)# Switch(config-i Switch(config-i Switch(config-i	Statically configured access ports can be configured with regular VLANs as guest y configured private VLAN host ports can be configured with secondary private VLANs. we how to enable a guest VLAN on Fast Ethernet interface 4/3: re terminal tion commands, one per line. End with CNTL/Z. interface fastethernet4/3 f)# dot1x port-control auto f)# dot1x guest-vlan 26 f)# end			
	VLAN host ports VLANs; statically VLANs as guest This example sho Switch# configura Switch(config)# Switch(config-i Switch(config-i	Statically configured access ports can be configured with regular VLANs as guest y configured private VLAN host ports can be configured with secondary private VLANs. we how to enable a guest VLAN on Fast Ethernet interface 4/3: re terminal tion commands, one per line. End with CNTL/Z. interface fastethernet4/3 f)# dot1x port-control auto f)# dot1x guest-vlan 26 f)# end			
Examples	VLAN host ports VLANs; statically VLANs as guest This example sho Switch# configura Switch(config)# Switch(config-i Switch(config-i Switch(config-i Switch(config)# Switch(config)#	. Statically configured access ports can be configured with regular VLANs as guest y configured private VLAN host ports can be configured with secondary private VLANs. we how to enable a guest VLAN on Fast Ethernet interface 4/3: re terminal tion commands, one per line. End with CNTL/Z. interface fastethernet4/3 f)# dot1x port-control auto f)# dot1x guest-vlan 26 f)# end end			
	VLAN host ports VLANs; statically VLANs; statically VLANs as guest This example sho Switch# configura Switch(config)# Switch(config-i Switch(config-i Switch(config-i Switch(config)# Switch(config)# Switch(config)# Switch	. Statically configured access ports can be configured with regular VLANs as guest y configured private VLAN host ports can be configured with secondary private VLANs. www.show.to.enable.a.guest VLAN on Fast Ethernet interface 4/3: reterminal tion commands, one per line. End with CNTL/Z. interface fastethernet4/3 f)# dot1x port-control auto f)# dot1x guest-vlan 26 f)# end end Description			
Examples	VLAN host ports VLANs; statically VLANs as guest This example sho Switch# configura Switch(config)# Switch(config-i Switch(config-i Switch(config-i Switch(config)# Switch(config)#	. Statically configured access ports can be configured with regular VLANs as guest y configured private VLAN host ports can be configured with secondary private VLANs. www.show.to.enable.a.guest VLAN on Fast Ethernet interface 4/3: reterminal tion commands, one per line. End with CNTL/Z. interface fastethernet4/3 f)# dot1x port-control auto f)# dot1x guest-vlan 26 f)# end end Description			

dot1x guest-vlan supplicant

To place an 802.1X-capable supplicant (host) into a guest VLAN, use the **dot1x guest-vlan supplicant** global configuration command. To return to the default setting, use the **no** form of this command.

dot1x quest-vlan supplicant

no dot1x quest-vlan supplicant

Syntax Description	This command has no arguments or keywords.			
Defaults	802.1X-capable hosts are not put into a guest VLAN.			
Command Modes	Global configuration mode			
Command History	Release	Modification		
-	12.2(25)EWA	Support for this comn	nand was introduced on the Catalyst 4500 series switch.	
Usage Guidelines	With Cisco Release 12.2(25) EWA, you can use the dot1x guest-vlan supplicant command to place an 802.1X-capable host into a guest VLAN. Prior to Cisco Release 12.2(25)EWA, you could only place non-802.1X capable hosts into a guest VLAN. When guest VLAN supplicant behavior is enabled, the Catalyst 4500 series switch does not maintain EAPOL packet history. The switch allows clients that fail 802.1X authentication to access a guest VLAN, whether or not EAPOL packets have been detected on the interface.			
Examples	This example shows how to place an 802.1X-capable supplicant (host) into a guest VLAN: Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# dot1x guest-vlan supplicant Switch(config)# end Switch#			
Related Commands	Command		Description	
	dot1x system-a	uth-control	Enables 802.1X authentication on the switch.	

Displays dot1x information.

show dot1x

dot1x host-mode

Use the **dot1x host-mode** interface configuration command on the switch stack or on a standalone switch to allow a single host (client) or multiple hosts on an IEEE 802.1x-authorized port. Use the **multi-domain** keyword to enable multidomain authentication (MDA) on an IEEE 802.1x-authorized port. Use the **no** form of this command to return to the default setting.

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

no dot1x host-mode [multi-host | single-host | multi-domain }

	·	
Syntax Description	multi-host	Enable multiple-hosts mode on the switch.
	single-host	Enable single-host mode on the switch.
	multi-domain	Enable MDA on a switch port.
Defaults	The default is sing	le-host mode.
Command Modes	Interface configura	tion mode
Command History	Release	Modification
	12.2(20)EWA	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(37)SG	Added support for multiple domains.
Usage Guidelines	an IEEE 802.1x-en successfully author	to limit an IEEE 802.1x-enabled port to a single client or to attach multiple clients to abled port. In multiple-hosts mode, only one of the attached hosts needs to be rized for all hosts to be granted network access. If the port becomes unauthorized fails or an Extensible Authentication Protocol over LAN [EAPOL]-logoff message is
	received), all attach	ned clients are denied access to the network.
	Use the multi-dom and a voice domain	ned clients are denied access to the network. ain keyword to enable MDA on a port. MDA divides the port into both a data domain n. MDA allows both a data device and a voice device, such as an IP phone (Cisco or same IEEE 802.1x-enabled port.

 Examples
 This example shows how to enable IEEE 802.1x authentication and to enable multiple-hosts mode:

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

 Switch(config)# interface gigabitethernet6/1
 Switch(config-if)# dot1x port-control auto

 Switch(config-if)# dot1x host-mode multi-host
 Switch(config-if)# dot1x host-mode multi-host

 Switch(config-if)# dot1x host-mode multi-host
 Switch(config-if)# end

 Switch#
 This example shows how to enable MDA and to allow both a host and a voice device on the port:

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

 Switch(config)# interface FastEthernet6/1
 Switch(config)# interface FastEthernet6/1

```
Switch(config)# interface FastEthernet6/1
Switch(config-if)# switchport access vlan 12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 10
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-domain
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch#
```

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

Related Commands	Command	Description
	show dot1x	Displays dot1x information.

dot1x initialize

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

dot1x initialize interface

Syntax Description	interface	Number of the interface.
Defaults	This command h	nas no default settings.
Command Modes	Privileged EXE	C mode
Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Usage Guidelines	Use this comma	nd to initialize state machines and to set up the environment for fresh authentication.
Examples	This example sh	nows how to initialize the 802.1X state machines on an interface:
	Switch# dot1x Switch#	initialize
Related Commands	Command	Description
	show dot1x	Displays dot1x information.

dot1x mac-auth-bypass

To enable the 802.1X MAC address bypassing on a switch, use the **dot1x mac-auth-bypass** command. Use the **no** form of this command to disable MAC address bypassing.

dot1x mac-auth-bypass [eap]

no dot1x mac-auth-bypass [eap]

Syntax Description	eap (Optional) Specifies using EAP MAC address authentication.	
Defaults	There is no defa	ault setting.
Command Modes	Interface config	guration mode
Command History	Release	Modification
	12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switch.
Usage Guidelines	The removal of the dot1x mac-auth-bypass configuration from a port does not affect the authorizat or authentication state of a port. If the port is in unauthenticated state, it remains unauthenticated, and MAB is active, the authentication will revert back to the 802.1X Authenticator. If the port is authorized with a MAC address, and the MAB configuration is removed the port remains authorized until re-authentication takes place. When re-authentication occurs the MAC address is removed in favor of 802.1X supplicant, which is detected on the wire.	
Examples	1	hows how to enable EAP MAC address authentication: -if)# dot1x mac-auth-bypass -if)#

dot1x max-reauth-req

To set the maximum number of times that 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		<i>count</i> 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 send	s a maximum of two retransmissions.		
Command Modes	Interface config	uration mode.		
Command History	Release	Modification		
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.		
Usage Guidelines	unreliable links setting impacts configured.	age the default value of this command only to adjust for unusual circumstances such as or specific behavioral problems with certain clients and authentication servers. This the wait before a non-dot1x-capable client is admitted to the guest VLAN, if one is your settings by entering the show dot1x privileged EXEC command.		
Examples	EAP-Request/Id	ows how to set 5 as the number of times that the switch retransmits an entity frame before restarting the authentication process: if)# dot1x max-reauth-reg 5 if)#		
Related Commands	Command	Description		
	show dot1x	Displays dot1x information.		

dot1x max-req

To set the maximum number of times that 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 send	ds a maximum of two retransmissions.	
Command Modes	Interface config	guration mode	
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	unreliable links	nge the default value of this command only to adjust for unusual circumstances such as or specific behavioral problems with certain clients and authentication servers. 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 frame before restarting the authentication process: Switch(config-if)# dot1x max-reg 5		
	Switch(config-if)#		
	1	hows how to return to the default setting: -if)# no dot1x max-req -if)#	

Related Commands	Command	Description
	dot1x initialize	Unauthorizes an interface before reinitializing 802.1X.
	dot1x max-reauth-req	Sets the maximum number of times that the switch will retransmit an EAP-Request/Identity frame to the client before restarting the authentication process.
	show dot1x	Displays dot1x information.

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-unauthorize	ed 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 at	uthorization is disabled.	
Command Modes	Interface configura	tion mode	
Command History	Release	Modification	
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.	
Usage Guidelines	-	ol is supported on both the Layer 2 static-access ports and the Layer 3-routed ports.	
	 You can use the auto keyword only if the port is not configured as follows: 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.		
	If you try to ch	hange the mode of an 802.1X-enabled port to dynamic, the port mode is not changed	
	• EtherChannel J EtherChannel. EtherChannel,	hange the mode of an 802.1X-enabled port to dynamic, the port mode is not changed. port—Before enabling 802.1X on the port, you must first remove it from the If you try to enable 802.1X on an EtherChannel or on an active port in an an error message appears, and 802.1X is not enabled. If you enable 802.1X on an f 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 the show dot1x all or show dot1x interface int commands 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
 Command
 Description

 show dot1x
 Displays dot1x information.

Γ

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 interface	<i>ace-id</i> (Optional) Module and port number of the interface.
Defaults	This command h	as no default settings.
Command Modes	Privileged EXEC	C mode
Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Jsage Guidelines		command to reauthenticate a client without waiting for the configured number of reauthentication attempts (re-authperiod) and automatic reauthentication.
Examples	This example sho interface 1/1:	ows how to manually reauthenticate the device connected to Gigabit Ethernet
		re-authenticate interface gigabitethernet1/1 nentication on gigabitethernet1/1

dot1x re-authentication

To enable the 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 mode

Command HistoryReleaseModification12.1(12c)EWSupport for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines You configure the amount of time between the periodic reauthentication attempts by using the dot1x timeout re-authperiod global configuration command.

Examples This example shows how to disable the periodic reauthentication of the client:

Switch(config-if)# no dot1x re-authentication
Switch(config-if)#

This example shows how to enable the periodic reauthentication and set the number of seconds between the 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	Command	Description
	dot1x timeout	Sets the reauthentication timer.
	show dot1x	Displays dot1x information.

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 mode

 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 the 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 the 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	Command	Description
	dot1x initialize	Unauthorizes an interface before reinitializing 802.1X.
	show dot1x	Displays dot1x information.

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 | server} | 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 seconds	Number of seconds between reauthentication attempts; valid values are from 1 to 65535. See the "Usage Guidelines" section for more information.		
	reauth-period server	Number of seconds between reauthentication attempts; valid values are from 1 to 65535 as derived from the Session-Timeout RADIUS attribute. See the "Usage Guidelines" section for more information.		
	quiet-period seconds	Number of seconds that 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 seconds	Number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request; valid values are from 1 to 65535 seconds. Number of seconds that the switch waits for the retransmission of EAP-Request packets; valid values are from 30 to 65535 seconds.		
	supp-timeout seconds			
	server-timeout <i>seconds</i> Number of seconds that the switch waits for the retransmission of packets by the back-end authenticator to the authentication server; values are from 30 to 65535 seconds.			
Defaults	The default settings are a	s follows:		
Delauns				
	• Reauthentication per	iod is 3600 seconds.		
	-			
	• Quiet period is 60 se	conds.		
	Quiet period is 60 seTransmission period	conds. is 30 seconds.		
	• Quiet period is 60 se	conds. is 30 seconds. s 30 seconds.		
Command Modes	 Quiet period is 60 se Transmission period Supplicant timeout is 	conds. is 30 seconds. s 30 seconds. seconds.		
Command Modes Command History	 Quiet period is 60 se Transmission period Supplicant timeout is Server timeout is 30 	conds. is 30 seconds. s 30 seconds. seconds.		
	 Quiet period is 60 se Transmission period Supplicant timeout is Server timeout is 30 Interface configuration m 	conds. is 30 seconds. s 30 seconds. seconds.		

Usage Guidelines	-	n must be enabled before entering the dot1x timeout re-authperiod e-authentication command to enable periodic reauthentication.		
Examples	*	set 60 as the number of seconds that the switch waits for a response to an from the client before retransmitting the request:		
	Switch# configure termina: Enter configuration comman Switch(config)# interface Switch(config-if)# dot1x f Switch(config-if)# end Switch#	nds, one per line. End with CNTL/Z. fastethernet4/3		
	You can verify your settings by entering the show dot1x privileged EXEC command.			
	This example shows how to set up the switch to use a reauthentication timeout derived from a Session-Timeout attribute taken from the RADIUS Access-Accept message received when a host successfully authenticates via 802.1X:			
	Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# interface fastethernet4/3 Switch(config-if)# dot1x timeout reauth-period server Switch(config-if)# end Switch#			
Related Commands	Command	Description		
	dot1x initialize	Unauthorizes an interface before reinitializing 802.1X.		

Displays dot1x information.

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

10/100/1000

Syntax Description	auto Specifie	s the autonegotiatio	n operation.	
	full Specifie	s the full-duplex op	eration.	
	half Specifie	s the half-duplex op	eration.	
Defaults	Half-duplex operation			
Command Modes	Interface configuratio	n mode		
Command History	Release Mo	odification		
	12.1(8a)EW Su	pport for this comm	and was introduced	d on the Catalyst 4500 series switch.
Usage Guidelines	Table 2-1 lists the sup	ported command op	otions by interface.	
	Table 2-1 Supp	orted duplex Comn	nand Options	
	Interface Type	Supported Syntax	Default Setting	Guidelines
	10/100-Mbps module	e 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.

duplex [half |

full]

duplex.

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**, the 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.

Caution

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

Table 2-2 describes the system performance for different combinations of the duplex and speed modes. The specified **duplex** command that is configured with the specified **speed** command produces the resulting action shown in the table.

Table 2-2	Relationship Between duplex and speed Commands
	neidilonship between duplex and speed ooninands

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

Command	Description	
speed	Configures the interface speed.	
interface (refer to Cisco IOS documentation)	Configures an interface.	
show controllers (refer to Cisco IOS documentation)	Displays controller information.	
show interfaces	Displays interface information.	

erase

To erase a file system, use the erase command.

erase {/all [non-default | nvram:] | cat4000_flash | nvram: | startup-config}

Syntax Description	/all nvram:	Erases everything in nvram:.
	/all non-default	Erases files and configuration in non-volatile storage including nvram:, bootflash:, cat4000_flash:, and crashinfo: of the local
		supervisor engine. Resets the Catalyst 4500 series switch to the
		factory default settings.
		Note This command option is intended to work only on a stand-alone supervisor engine.
	cat4000_flash:	Erases the VLAN database configuration file.
	nvram:	Erases the startup-config and private-config file in nvram.
	startup-config:	Erases the startup-config and private-config file in nvram.
Defaults	This command has	s no default settings.
Command Modes	Privileged EXEC 1	mode
Command History	Release	Modification
	12.2(25)SG	Support for this command was introduced on the Catalyst 4500 series switch.
Usage Guidelines		
Caution	When you use the	erase command to erase a file system, you cannot recover the files in the file system.
	nvram: and flash (command options shown above, options with the prefix slave that are used to identify like slavenvram: and slavecat4000_flash:) appear in the command help messages on r redundancy switch.
		command replaces the write erase and the erase startup-confg commands. Like ads, it erases both the startup-config and the private-config file.
	The erase /all nvr private-config file.	am: command erases all files in nvram: in addition to startup-config file and
	The erase cat4000	_flash: command erases the VLAN database configuration file.
	It erases the config	-default command facilitates the work of a manufacturing facility and repair center. guration and states stored in the non-volatile storage and resets the Catalyst 4500 series ary default settings. The default settings include those mentioned in the IOS library

It erases the configuration and states stored in the non-volatile storage and resets the Catalyst 4500 series switch to the factory default settings. The default settings include those mentioned in the IOS library (below) as well as those set by the **erase /all non-default** command (vtp mode=transparent, and the ROMMON variables: ConfigReg=0x2101, PS1= "rommon ! >" and EnableAutoConfig=1).

- Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2, at this URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fun_c/index.htm
- Cisco IOS Configuration Fundamentals Configuration Command Reference, Release 12.2, at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fun_r/index.htm

Caution

n The erase /all non-default command can erase IOS images in bootflash:. Ensure that 1) an IOS image can be copied back to the bootflash: (such as, from a accessible TFTP server or a flash card inserted in slot0: (available on most chassis models), or 2) the switch can boot from a image stored in an accessible network server.

Examples

This example shows how to erase the files and configuration in a non-volatile storage and reset the switch to factory default settings:

EnableAutoConfig=1 Setting vtp mode to transparent %WARNING! Please reboot the system for the changes to take effect Switch# 00:01:48: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram Switch#

This example shows how to erase the contents in nvram.

PS1=rommon ! >

```
Switch# erase /all nvram:
Erasing the nvram filesystem will remove all files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
00:38:10: %SYS-7-NV_BLOCK_INIT: Initalized the geometry of nvram
Switch#
```

This example shows how to erase filesystem cat4000_flash.

```
Switch# erase cat4000_flash:
Erasing the cat4000_flash filesystem will remove all files! Continue? [confirm]
[OK]
Erase of cat4000_flash:complete
Switch#
```

Related Commands	Command	Description
	boot config (refer to Cisco IOS documentation)	Specifies the device and filename of the configuration file.
	delete (refer to Cisco IOS documentation)	Deletes a file from a Flash memory device or NVRAM.
	show bootvar	Displays BOOT environment variable information.
	undelete (refer to Cisco IOS documentation)	Recovers a file marked "deleted" on a Class A Flash file system.

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 the detection for the ARP inspection error-disable cause.
	dhcp-rate-limit	Specifies the detection for the DHCP rate-limit error-disable cause.
	dtp-flap	Specifies the detection for the DTP flap error-disable cause.
	gbic-invalid	Specifies the detection for the GBIC invalid error-disable cause.
	l2ptguard	Specifies the detection for the Layer 2 protocol-tunnel error-disable cause.
	link-flap	Specifies the detection for the link flap error-disable cause.
	pagp-flap	Specifies the detection for the PAgP flap error-disable cause.
Defaults	All error-disable of	causes are detected.
Command Modes	Global configurat	ion mode
	ereeur vonnigurui	
Command History	Release	Modification
	12.1(8a)EW	Summent for this command was introduced on the Catalyst 4500 conies switch
		Support for this command was introduced on the Catalyst 4500 series switch.
		Support for this command was introduced on the Cataryst 4500 series switch.
Usage Guidelines	When a cause is d	link-flap, pagp-flap) is defined as the reason why the error-disabled state occurred. etected on an interface, the interface is placed in error-disabled state (an operational r to link-down state).
Usage Guidelines	When a cause is d state that is simila You must enter th	link-flap, pagp-flap) is defined as the reason why the error-disabled state occurred. etected on an interface, the interface is placed in error-disabled state (an operational
Usage Guidelines	When a cause is d state that is simila You must enter th manually from the	link-flap, pagp-flap) is defined as the reason why the error-disabled state occurred. etected on an interface, the interface is placed in error-disabled state (an operational r to link-down state). e shutdown command and then the no shutdown command to recover an interface

Switch#

This example shows how to disable error-disable detection for DAI:

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 12ptguard Enabled gbic-invalid Enabled dhcp-rate-limit Enabled unicast-flood Enabled storm-control Enabled Enabled ilpower arp-inspection Disabled

Related Commands

Command	Description
show errdisable detect	Displays the error disable detection status.
show interfaces status	Displays the interface status or a list of interfaces in error-disabled state.

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 | pesecure-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 | pescure-violation | security-violation | storm-control | udld | unicastflood | vmps} [arp-inspection] [interval {*interval*}]]

Syntax Description	cause	(Optional) Enables the 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.
	pesecure-violation	(Optional) Enables the recovery timer for the pesecure violation error-disable cause.
	security-violation	(Optional) Enables the automatic recovery of ports disabled due to 802.1X security violations.
	storm-control	(Optional) Enables the 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 the ARP inspection cause and recovery timeout.
	interval interval	(Optional) Specifies the time to recover from a specified error-disable cause; valid values are from 30 to 86400 seconds.

Defaults	Error disable recovery is disabled.		
	The recovery interva	al is set to 300 seconds.	
Command Modes	Configuration		
Command History	Release	Addification	
-	12.1(8a)EW S	Support for this command was introduced on the Catalyst 4500 series switch.	
		Support for the storm-control feature.	
Usage Guidelines	state occurred. Whe (an operational state for the cause, the in you enable recovery	, dtp-flap, link-flap, pagp-flap, udld) is defined as the reason why the error-disabled n a cause is detected on an interface, the interface is placed in error-disabled state e that is similar to the link-down state). If you do not enable error-disable recovery terface stays in the error-disabled state until a shutdown and no shutdown occurs. If for a cause, the interface is brought out of the error-disabled state and allowed to n 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)#		
	This example shows how to enable the errdisable recovery for arp-inspection:		
	Switch(config)# e: Switch(config)# er Switch# show errd : ErrDisable Reason		
	udld bpduguard security-violatio channel-misconfig	Disabled Disabled Disabled Disabled Disabled	
	vmps pagp-flap dtp-flap	Disabled Disabled Disabled	
	link-flap l2ptguard psecure-violation gbic-invalid	Disabled Disabled Disabled Disabled	
	dhcp-rate-limit unicast-flood storm-control arp-inspection	Disabled Disabled Disabled Enabled	

Timer interval: 300 seconds Interfaces that will be enabled at the next timeout: Switch#

Related Commands

Command	Description	
show errdisable detect	Displays the error disable detection status.	
show errdisable recovery	Displays error disable recovery timer information.	
show interfaces status	Displays the interface status or a list of interfaces in error-disabled state.	

Catalyst 4500 Series Switch Cisco IOS Command Reference—Release 12.2(46)SG

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.	
offPrevents a local port from receiving and processing pause frames from from sending pause frames to remote ports.		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 pause frames to remote ports.		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 off—non-oversubscribed Gigabit Ethernet interfaces.
- Receiving pause frames is desired—non-oversubscribed Gigabit Ethernet interfaces.
- Sending pause frames is on—Oversubscribed Gigabit Ethernet interfaces.
- Receiving pause frames is desired—Oversubscribed Gigabit Ethernet interfaces

Table 2-3 shows the default settings for the modules.

Table 2-3Default Module Settings

Module	Ports	Send
All modules except WS-X4418-GB and WS-X4416-2GB-TX	All ports except for the oversubscribed ports	Off
WS-X4418-GB	Uplink ports (1–2)	Off
WS-X4418-GB	Oversubscribed ports (3–18)	On
WS-X4412-2GB-TX	Uplink ports (13–14)	Off
WS-X4412-2GB-TX	Oversubscribed ports (1–12)	On
WS-X4416-2GB-TX	Uplink ports (17–18)	Off

Command Modes Interface configuration mode

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

Usage Guidelines The pause frames are special packets that signal a source to stop sending frames for a specific period of time because the buffers are full.

Table 2-4 describes the guidelines for using the different configurations of the **send** and **receive** keywords with the **flowcontrol** command.

Table 2-4Keyword 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 a 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 .	

Table 2-5 identifies how the flow control will be forced or negotiated on the Gigabit Ethernet interfaces based on their speed settings.

Table 2-5 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

Command	Description	
interface port-channel	Accesses or creates a port-channel interface.	
interface range	Runs a command on multiple ports at the same time.	
show flowcontrol	Displays the per-interface status and statistics related to flow control.	
show running-config	Displays the running-configuration for a switch.	
speed Configures the interface speed.		

hardware statistics

To enable TCAM hardware statistics in your ACLs use the **hardware statistics** command. To disable TCAM hardware statistics, use the **no** form of this command.

hardware statistics

no hardware statistics

- **Syntax Description** This command has no arguments or keywords.
- **Defaults** Hardware statistics is disabled.
- **Command Modes** Global configuration mode

 Release
 Modification

 12.2(40)SG
 Support for the Supervisor Engine 6-E and Catalyst 4900M chassis is introduced.

Usage Guidelines The Supervisor Engine 6-E and Catalyst 4900M chassis TCAM hardware does not have enough hardware statistics entries for every classification/QoS cam entry. Therefore, the statistics for each cam entry needs to be enabled as needed.

Examples This example shows how to enable TCAM hardware statistics in your ACLs ace: Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#ip access-list extended myv4 Switch(config-ext-nacl)#permit ip any any Switch(config-ext-nacl)#hardware statistics Switch(config-ext-nacl)#end

Related Commands	Command	Description
	ip access list (refer to Cisco IOS documentation)	Creates an IP ACL (Access Control List).
	ipv6 access list (refer to Cisco IOS documentation)	Creates an IPv6 ACL.
	mac access-list extended	Defines the extended MAC access lists.
hw-module port-group

To select either Gigabit Ethernet or Ten Gigabit Ethernet interfaces on your module, use the **hw-module port-group** command.

hw-module *module number* **port-group** *number* **select** [gigabitethernet | tengigabitethernet]

Syntax Description	module	Specifies a line module.	
	number	Specifies a module which supports TwinGig converter.	
	port-group number	Port-group number on a switch.	
	select	Specifies an interface type; valid values are Gigabit Ethernet and 10-Gigabit Ethernet.	
	gigabitethernet	(Optional) Specifies Gigabit Ethernet.	
	tengigabitethernet	(Optional) Specifies 10-Gigabit Ethernet.	
Defaults	10 Gigabit.		
Command Modes	Global configuration mo	ode	
Command History	Release Modification		
	12.2(40)SG Supp	ort for TwinGig converter module introduced.	
Usage Guidelines Examples	 Support for this command is available on the Cisco Catalyst 4500 modules that support TwinGig converter modules. Such as, the Supervisor Engine 6-E and WS-X4606-10GE-E. This example shows how to select Gigabit Ethernet interfaces on a WS-X4606-10GE-E using the second select Gigabit Ethernet interfaces on a WS-X4606-10GE-E using the second select Gigabit Ethernet interfaces on a WS-X4606-10GE-E using the second select Gigabit Ethernet interfaces on a WS-X4606-10GE-E using the second select Gigabit Ethernet interfaces on a WS-X4606-10GE-E using the second select Gigabit Ethernet interfaces on a WS-X4606-10GE-E using the second select Gigabit Ethernet interfaces on a WS-X4606-10GE-E using the second select Gigabit Ethernet interfaces on a WS-X4606-10GE-E using the second select Gigabit Ethernet interfaces on a WS-X4606-10GE-E using the second select Gigabit Ethernet interfaces on a WS-X4606-10GE-E using the second select Gigabit Ethernet interfaces on a WS-X4606-10GE-E using the second select Gigabit Ethernet interfaces on a WS-X4606-10GE-E using the second select Gigabit Ethernet interfaces on a WS-X4606-10GE-E using the second select Gigabit Ethernet interfaces on a WS-X4606-10GE-E using the second select Gigabit Ethernet interfaces on a WS-X4606-10GE-E using the second select Gigabit Ethernet interfaces on a WS-X4606-10GE-E using the second select Gigabit Ethernet interfaces on a WS-X4606-10GE-E using the second select Gigabit Ethernet interfaces on a WS-X4606-10GE-E using the second select Gigabit Ethernet interfaces on a WS-X4606-10GE-E using the second select Gigabit Ethernet interfaces on a WS-X4606-10GE-E using the second select Gigabit Ethernet interfaces on a WS-X4606-10GE-E using the second select Gigabit Ethernet interfaces on a WS-X4606-10GE-E using the second select gigabit second select gigabit second second		
•	TwinGig Converter:		
	Switch# config terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# hw-module module 1 port-group 1 select gigabitethernet Switch(config)# exit		
	Use the show interfaces	s status command to display your configuration.	
Related Commands	Command	Description	
	show hw-module port-	-group Displays how the X2 holes on a module are grouped.	
	show interfaces status		

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) Slot or module number.
Defaults	After a boot up	the power is on.	
ommand Modes	Global configu	ration mode	
Command History	Release	Modification	
	12.1(8a)EW	Support for this co	mmand was introduced on the Catalyst 4500 series switch.
	12.2(18)EW	Add slot and modu	le keywords.
Examples	This example sl	nows how to shut off p	ower to a module in slot 5:
	Switch# no hw - Switch#	module slot 5 power	
Related Commands	Command		Description
	clear hw_mod	ule slot password	Clears the password on an intelligent line module.

hw-module uplink mode shared-backplane

	the Supervisor Engine 6-E and Catalyst 4900M chassis when operating in redundant mode, use the hw-module uplink mode shared-backplane command.		
	To disable shared-backplane uplink mode, use the no form of the command.		
	[no] hw-module uplink mode shared-backplane		
Syntax Description	This command has no keywords or arguments.		
Defaults	Only two Ten-Gigabit Ethernet ports OR four One-Gigabit Ethernet ports can be used on the supervisor engine.		
Command Modes	Global configuration mode		
Command History	Release Modification		
	12.2(44)SGSupport for this command was introduced on the Catalyst 4500 series switch.		
Usage Guidelines	When changing the uplink mode using the hw-module uplink mode shared-backplane command, you must reload the system. A message is printed on the console to reflect this.		
Examples	This example shows how to enable shared-backplane uplink mode:		
	Switch(config)# hw-module uplink mode shared-backplane A reload of the active supervisor is required to apply the new configuration. Switch(config)# exit Switch#		
	This example shows how to disable shared-backplane uplink mode:		
	Switch(config)# no hw-module uplink mode shared-backplane A reload of the active supervisor is required to apply the new configuration. Switch(config)# exit Switch#		
	This example shows how to display the current state of uplink-mode:		
	Switch# show hw-module uplink Active uplink mode configuration is Default (will be Shared-backplane after next reload)		
	A reload of active supervisor is required to apply the new configuration.		

To change the uplink mode so that you can use all four Ten-Gigabit Ethernet ports as blocking ports on

Related Commands	Command	Description
	show hw-module uplink	Displays hw-module uplink information.

up in the new uplink mode.

hw-module uplink select

To select the 10-Gigabit Ethernet or Gigabit Ethernet uplinks on the Supervisor Engine V-10GE within the W-C4510R chassis, use the **hw-module uplink select** command.

hw-module uplink select {tengigabitethernet | gigabitethernet | all}

Syntax Description	tengigabitethe	ernet (Optional) Specifies the 10-Gigabit Ethernet uplinks.
	gigabitetherne	
	all	(Optional) Specifies all uplinks (10-Gigabit Ethernet and Gigabit Ethernet).
Defaults	tengigabitether	net
Command Modes	Global configu	ration mode
Command History	Release	Modification
	12.2(25)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(25)SG	Support for the all keyword was added.
Usage Guidelines	if a startup conf cycled, the syst with the new up	r Engine V-10GE (WS-X4516-10GE) in a 10 slot chassis (Catalyst 4510R and 4510R-E), figuration with a new uplink mode is copied into flash memory and the system is power em will not come up with the new uplink mode. After copying the startup configuration blink mode into flash memory, the uplink mode must be changed to the new uplink mode nmand interface before the system is power cycled. This ensures that the system comes

Supervisor Engine V-10GE and Supervisor Engine II+10GE support 10-Gigabit Ethernet and Gigabit Ethernet uplink ports. On the Supervisor Engine II+10GE, all uplink ports are always available. Similarly, when a Supervisor Engine V-10GE is plugged into a W-C4503, W-4506, or W-4507R chassis, all uplink ports are always available. When a Supervisor Engine V-10GE is plugged into a W-4510R chassis, you can choose to use the 10-Gigabit Ethernet uplink ports, the Gigabit Ethernet uplink ports, or all uplink ports. If you choose to use all uplink ports, then the tenth slot will support only the WS-X4302-GB switching linecard. Be aware that this command takes effect only after a reload (after you have executed the **redundancy reload shelf** command).

Because the uplink selection is programmed into hardware during initialization, changing the active uplinks requires saving the configuration and reloading the switch. When you are configuring a change to the uplinks, the system responds with a message informing you that the switch must be reloaded and suggesting the appropriate command (depending on redundancy mode) to reload the switch.

If you select the **all** keyword, ensure that the tenth slot is either empty or has a WS-X4302-GB switching module.

A no form of this command does not exist. To undo the configuration, you must configure the uplinks.

Γ

	Note	If you select the all keyword, only the Drome board will be supported in the tenth slot of the supervise engine.
		Switch(config)# exit Switch#
		A 'redundancy reload shelf' or power-cycle of chassis is required to apply the new configuration.
		Switch(config)# hw-module uplink select all Warning: This configuration mode may disable slot10.
		This example shows how to select all the uplinks in a redundant system in SSO mode:
	Note	The Gigabit Ethernet uplinks will be active on a switchover or reload of the active supervisor engine
		Switch#
		A reload of the active supervisor is required to apply the new configuration. Switch(config)# exit
		Switch(config)# hw-module uplink select gigabitethernet
		This example shows how to select the Gigabit Ethernet uplinks in a redundant system in RPR mode:
	Note	The Gigabit Ethernet uplinks will be active after the next reload of the chassis/shelf. Use the redundancy reload shelf command to reload the chassis/shelf.
	Netr	The Circulat Ethemat unlinks will be active often the next related of the charge of the Hard the
		Switch(config)# exit Switch#
		A 'redundancy reload shelf' or power-cycle of chassis is required to apply the new configuration
		Switch(config)# hw-module uplink select gigabitethernet
		This example shows how to select the Gigabit Ethernet uplinks in a redundant system in SSO mode:
	Note	The Gigabit Ethernet uplinks will be active after the next reload.
		Switch#
		A reload of the active supervisor is required to apply the new configuration. Switch(config)# exit
•		Switch(config)# hw-module uplink select gigabitethernet
Examples		This example shows how to select the Gigabit Ethernet uplinks:

Displays hw-module uplink information.

show hw-module uplink

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 {vlans vlan-range}

no instance instance-id

from 0 to 15. vlans vlan-range Specifies the number of the VLANs to be mapped to the specifies the number is entered as a single value or a range; valid value 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 ser Usage Guidelines The mapping is incremental, not absolute. When you enter a range of VLANs, this range removed to the existing ones. Any unmapped VLAN is mapped to the CIST instance. Switch(config-mst) # instance 2 vlans 1-100 Switch(config-mst) # Examples This example shows how to map a range of VLANs to instance 5: Switch(config-mst) # Switch(config-mst) # instance 5 vlans 1100 Switch(config-mst) #				
The number is entered as a single value or a range; valid value 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 set Usage Guidelines The mapping is incremental, not absolute. When you enter a range of VLANs, this range 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) # This example shows how to move a range of VLANs from instance 2 to the CIST instance Switch(config-mst) # This example shows how to move a range of VLANs from instance 2 to the CIST instance Switch(config-mst) # This example shows how to move a range of VLANs from instance 2 to the CIST instance Switch(config-mst) # This example shows how to move all the VLANs mapped to instance 2 back to the CIST switch(config-mst) #	Syntax Description	instance-id	MST instance to which the specified VLANs are mapped; valid values are from 0 to 15.	
Command Modes MST configuration Command History Release Modification 12.1(12c)EW Support for this command was introduced on the Catalyst 4500 set Usage Guidelines The mapping is incremental, not absolute. When you enter a range of VLANs, this range 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) # This example shows how to move a range of VLANs from instance 2 to the CIST instance Switch(config-mst) # This example shows how to move a range of VLANs from instance 2 to the CIST instance Switch(config-mst) # This example shows how to move a range of VLANs from instance 2 to the CIST instance Switch(config-mst) # This example shows how to move all the VLANs mapped to instance 2 back to the CIST switch(config-mst) # no instance 2		vlans vlan-range	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.	
Command History Release Modification 12.1(12c)EW Support for this command was introduced on the Catalyst 4500 ser Usage Guidelines The mapping is incremental, not absolute. When you enter a range of VLANs, this range 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)# This example shows how to move a range of VLANs from instance 2 to the CIST instance Switch(config-mst)# This example shows how to move a range of VLANs from instance 2 to the CIST instance Switch(config-mst)# This example shows how to move a range of VLANs from instance 2 to the CIST instance 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 Switch(config-mst)# no instance 2	Defaults	Mapping is disabled		
12.1(12c)EW Support for this command was introduced on the Catalyst 4500 set Usage Guidelines The mapping is incremental, not absolute. When you enter a range of VLANs, this range removed to the existing ones. Any unmapped VLAN is mapped to the CIST instance. 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 switch(config-mst)#	Command Modes	MST configuration		
Usage Guidelines The mapping is incremental, not absolute. When you enter a range of VLANs, this range 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)# This example shows how to move a range of VLANs from instance 2 to the CIST instance Switch(config-mst)# This example shows how to move a range of VLANs from instance 2 to the CIST instance Switch(config-mst)# This example shows how to move a range of VLANs from instance 2 to the CIST instance Switch(config-mst)# This example shows how to move all the VLANs mapped to instance 2 back to the CIST switch(config-mst)# no instance 2	Command History	Release	Modification	
Usage Guidelines The mapping is incremental, not absolute. When you enter a range of VLANs, this range 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)# This example shows how to move a range of VLANs from instance 2 to the CIST instance Switch(config-mst)# This example shows how to move a range of VLANs from instance 2 to the CIST instance Switch(config-mst)# This example shows how to move a range of VLANs from instance 2 to the CIST instance Switch(config-mst)# This example shows how to move all the VLANs mapped to instance 2 back to the CIST Switch(config-mst)# This example shows how to move all the VLANs mapped to instance 2 back to the CIST Switch(config-mst)# no instance 2	-	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.	
 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 Switch(config-mst)# no instance 2 				
<pre>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 Switch(config-mst)# no instance 2</pre>	Examples	This example shows	how to map a range of VLANs to instance 2:	
<pre>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 Switch(config-mst)# no instance 2</pre>				
<pre>Switch(config-mst)# This example shows how to move a range of VLANs from instance 2 to the CIST instand 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 Switch(config-mst)# no instance 2</pre>		This example shows how to map a VLAN to instance 5:		
<pre>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 Switch(config-mst)# no instance 2</pre>				
Switch(config-mst)# This example shows how to move all the VLANs mapped to instance 2 back to the CIST Switch(config-mst)# no instance 2		This example shows how to move a range of VLANs from instance 2 to the CIST instance:		
Switch(config-mst)# no instance 2				
		This example shows	how to move all the VLANs mapped to instance 2 back to the CIST instance:	

mmands	Command	Description
	name	Sets the MST region name.
	revision	Sets the MST configuration revision number.
	show spanning-tree mst	Displays MST protocol information.
	spanning-tree mst configuration	Enters the MST configuration submode.

interface

To select an interface to configure and to enter interface configuration mode, use the **interface** command.

interface type number

Syntax Description	type	Type of interface to be configured; see Table 2-6 for valid values.	
- /	number	Module and port number.	
		·	
Defaults	No interface types are configured.		
Command Modes	Global configuration mode		
Command History	Release	Modification	
	12.2(25)EW	Extended to include the 10-Gigabit Ethernet interface.	
	Table 2-6 Keyword	Valid type Values	
	ethernet	Ethernet IEEE 802.3 interface.	
	fastethernet	100-Mbps Ethernet interface.	
	gigabitethern		
	tengigabitethe	ernet 10-Gigabit Ethernet IEEE 802.3ae interface.	
	ge-wan	Gigabit Ethernet WAN IEEE 802.3z interface; supported on Catalyst 4500 series switches that are configured with a Supervisor Engine 2 only.	
	pos	Packet OC-3 interface on the Packet over SONET Interface Processor; supported on Catalyst 4500 series switches that are configured with a Supervisor Engine 2 only.	
	atm	ATM interface; supported on Catalyst 4500 series switches that are configured with a Supervisor Engine 2 only.	
	vlan	VLAN interface; see the interface vlan command.	
	port-channel	Port channel interface; see the interface port-channel command.	

 Examples
 This example shows how to enter the interface configuration mode on the Fast Ethernet interface 2/4:

 Switch(config)# interface fastethernet2/4

 Switch(config-if)#

Related Commands	Command	Description
	show interfaces	Displays interface information.

interface port-channel

To access or create a port-channel interface, use the **interface port-channel** command.

interface port-channel channel-group

Suntax Description		Dert shared around an unlider here are form 1 to (4
Syntax Description	channel-group	Port-channel group number; valid values are from 1 to 64.
Defaults	This command h	as no default settings.
Command Modes	Global configura	ition mode
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.	
	a Layer 3 port cl switchport com	ate the port channels by entering the interface port-channel command. This will create nannel. To change the Layer 3 port channel into a Layer 2 port channel, use the mand before you assign the physical interfaces to the channel group. A port channel ed from Layer 3 to Layer 2 or vice versa when it contains member ports.
	Only one port ch	nannel in a channel group is allowed.
$\underline{\wedge}$		
Caution		t-channel interface is the routed interface. Do not enable Layer 3 addresses on the hernet interfaces.
	If you want to us the port-channel	se CDP, you must configure it only on the physical Fast Ethernet interface and not on interface.
Examples	This example cro	eates a port-channel interface with a channel-group number of 64:
	Switch(config) Switch(config)	# interface port-channel 64 #
Related Commands	Command	Description
	channel-group	Assigns and configures an EtherChannel interface to an EtherChannel group.
	show etherchan	Displays EtherChannel information for a channel.

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}

yntax Description	vlan vlan_id - vlan_	<i>id</i> Specifies a VLAN range; valid values are from 1 to 4094.	
	port-range	Port range; for a list of valid values for <i>port-range</i> , see the "Usage Guidelines" section.	
	macro name	Specifies the name of a macro.	
efaults	This command has n	o default settings.	
ommand Modes	Global configuration mode		
	Interface configurati	on mode	
command History	Release N	lodification	
•••••••			
······	12.1(8a)EW S	upport for this command was introduced on the Catalyst 4500 series switch.	
	12.1(12c)EWSYou can use the inter	upport for extended VLAN addresses added. face range command on the existing VLAN SVIs only. To display the VLAN SVIs	
	12.1(12c)EW S You can use the inter enter the show runn interface range com	upport for extended VLAN addresses added. face range command on the existing VLAN SVIs only. To display the VLAN SVIs ing config command. The VLANs that are not displayed cannot be used in the	
	12.1(12c)EWSYou can use the inter enter the show runn interface range com The values that are e SVIs.	upport for extended VLAN addresses added. face range command on the existing VLAN SVIs only. To display the VLAN SVIs ing config command. The VLANs that are not displayed cannot be used in the mand.	
	12.1(12c)EWSYou can use the inter enter the show runn interface range com The values that are e SVIs.Before you can use a All configuration character	upport for extended VLAN addresses added. face range command on the existing VLAN SVIs only. To display the VLAN SVIs ing config command. The VLANs that are not displayed cannot be used in the imand. Intered with the interface range command are applied to all the existing VLAN	
	12.1(12c)EWSYou can use the inter enter the show runn interface range com The values that are e SVIs.Before you can use a All configuration cha are created with the s	upport for extended VLAN addresses added. "face range command on the existing VLAN SVIs only. To display the VLAN SVIs ing config command. The VLANs that are not displayed cannot be used in the mand. Intered with the interface range command are applied to all the existing VLAN a macro, you must define a range using the define interface-range command. anges that are made to a port range are saved to NVRAM, but the port ranges that	
	12.1(12c)EWSYou can use the inter enter the show runn interface range com The values that are e SVIs.Before you can use a All configuration cha are created with the s	upport for extended VLAN addresses added. face range command on the existing VLAN SVIs only. To display the VLAN SVIs ing config command. The VLANs that are not displayed cannot be used in the mand. Intered with the interface range command are applied to all the existing VLAN are macro, you must define a range using the define interface-range command. Intereface range command do not get saved to NVRAM, but the port ranges that interface range command do not get saved to NVRAM.	
	12.1(12c)EWSYou can use the inter enter the show runn interface range com The values that are e SVIs.Before you can use a All configuration cha are created with the You can enter the po • Specifying up to	upport for extended VLAN addresses added. face range command on the existing VLAN SVIs only. To display the VLAN SVIs ing config command. The VLANs that are not displayed cannot be used in the mand. Intered with the interface range command are applied to all the existing VLAN a macro, you must define a range using the define interface-range command. Interface range command do not get saved to NVRAM, but the port ranges that interface range command do not get saved to NVRAM. Interface range in two ways:	
	12.1(12c)EWSYou can use the inter enter the show runn interface range com The values that are e SVIs.Before you can use a All configuration cha are created with the figure You can enter the po • Specifying up to • Specifying a pre You can either specific	upport for extended VLAN addresses added. face range command on the existing VLAN SVIs only. To display the VLAN SVIs ing config command. The VLANs that are not displayed cannot be used in the mand. Intered with the interface range command are applied to all the existing VLAN a macro, you must define a range using the define interface-range command. anges that are made to a port range are saved to NVRAM, but the port ranges that interface range command do not get saved to NVRAM. rt range in two ways: o five port ranges	
	12.1(12c)EWSYou can use the inter enter the show runn interface range com The values that are e SVIs.Before you can use a All configuration cha are created with the b You can enter the po • Specifying up to • Specifying a pre You can either specif port type, and the po	upport for extended VLAN addresses added. "face range command on the existing VLAN SVIs only. To display the VLAN SVIs ing config command. The VLANs that are not displayed cannot be used in the umand. Intered with the interface range command are applied to all the existing VLAN a macro, you must define a range using the define interface-range command. anges that are made to a port range are saved to NVRAM, but the port ranges that interface range command do not get saved to NVRAM. rt range in two ways: o five port ranges wiously defined macro Y the ports or the name of a port-range macro. A port range must consist of the same	
sage Guidelines	12.1(12c)EWSYou can use the inter enter the show runn interface range com The values that are e SVIs.Before you can use a All configuration cha are created with the b You can enter the po • Specifying up to • Specifying a pre You can either specif port type, and the po You can define up to	Face range command on the existing VLAN SVIs only. To display the VLAN SVIs ing config command. The VLANs that are not displayed cannot be used in the umand. Intered with the interface range command are applied to all the existing VLAN a macro, you must define a range using the define interface-range command. Interface range command do not get saved to NVRAM, but the port ranges that interface range command do not get saved to NVRAM. Interface range in two ways: In five port ranges In two ways: In the port range in two ways: In the port range macro. A port range must consist of the same rts within a range cannot span the modules.	

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. 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 macro1

 Switch(config-if)#

 Related Commands
 Command
 Description

 define interface-range
 Creates a macro of interfaces.

 show running config (refer to Cisco IOS)
 Displays the running configuration for a switch

show running config (refer to Cisco IOS Displays the running configuration for a switch. 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*

	<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 mode			
Command History				
	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.		
	displayed when			
	ISL or 802.1Q-encapsulated trunk or the VLAN ID that is configured for an access por displayed whenever a VLAN interface is newly created, so you can check that you enter VLAN number.			
		SVI by entering the no interface vlan <i>vlan_id</i> command, the associated interface is		
	If you delete an forced into an ac	SVI by entering the no interface vlan <i>vlan_id</i> command, the associated interface is dministrative down state and marked as deleted. The deleted interface will no longer be v interface command.		
	If you delete an forced into an ac visible in a shov You can reinstat	dministrative down state and marked as deleted. The deleted interface will no longer be		
Examples	If you delete an forced into an ac visible in a shov You can reinstat interface. The ir	dministrative down state and marked as deleted. The deleted interface will no longer be w interface command. The a deleted SVI by entering the interface vlan <i>vlan_id</i> command for the deleted		

ip arp inspection filter vlan

To permit ARPs from hosts that are 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. To disable this application, use the **no** form of this command.

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	arp-acl-name	Access control list name.
	vlan-range	VLAN number or range; valid values are from 1 to 4094.
	static	(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	containing only th are bridged in the	cess control list is applied to a VLAN for dynamic ARP inspection, the ARP packets the IP-to-Ethernet MAC bindings are compared against the ACLs. All other packet types incoming VLAN without validation.
	-	becifies that the incoming ARP packets are compared against the ARP access control ets are permitted only if the access control list permits them.
		rol lists deny the packets because of explicit denies, the packets are dropped. If the d because of an implicit deny, they are then matched against the list of DHCP bindings applied statically.
Examples	This example sho	ws how to apply the ARP ACL "static-hosts" to VLAN 1 for DAI:
	Switch(config)# Switch(config)# Switch# Switch# show ip	tion commands, one per line. End with CNTL/Z. ip arp inspection filter static-hosts vlan 1 end arp inspection vlan 1
	Source Mac Valio Destination Mac IP Address Valio	Validation : Disabled

Vlan	Configuration	Operation	ACL Match	Static ACL
1	Enabled	Active	static-hosts	No
Vlan	ACL Logging	DHCP Loggin	ıg	
			-	
1	Acl-Match	Deny		
Switch#				

Related Commands

Command	Defines an ARP access list or adds clauses at the end of a predefined list.	
arp access-list		
show ip arp inspection	Displays the status of dynamic ARP inspection for a specific range of VLANs.	

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 the event of a DoS attack, use the **ip arp inspection limit** command. To release the limit, use the **no** form of this command.

ip arp inspection limit {rate *pps* | **none} [burst interval** *seconds*]

no ip arp inspection limit

Syntax Description	rate pps	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 the incoming ARP packets that can be processed.	
	burst interval seconds	(Optional) Specifies the consecutive interval in seconds over which the interface is monitored for the high rate of the ARP packets. The interval is configurable from 1 to 15 seconds.	
Defaults	The rate is set to 15 packets per second on the 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 or	n all the trusted interfaces.	
	The burst interval is set	t to 1 second by default.	
Command Modes	Interface		
Command History	Release N	Addification	
Command History		Nodification upport for this command was introduced on the Catalyst 4500 series switch.	
Command History	12.1(19)EW S	upport for this command was introduced on the Catalyst 4500 series switch.	
Command History	12.1(19)EW S		
Command History	12.1(19)EW S	upport for this command was introduced on the Catalyst 4500 series switch.	
	12.1(19)EWS12.1(20)EWAThe trunk ports should l incoming packets exceet The error-disable timeo applies to both the trusted	upport for this command was introduced on the Catalyst 4500 series switch. Added support for interface monitoring. be configured with higher rates to reflect their aggregation. When the rate of the eds the user-configured rate, the interface is placed into an error-disabled state. but feature can be used to remove the port from the error-disabled state. The rate	
Command History Usage Guidelines	12.1(19)EWS12.1(20)EWAThe trunk ports should l incoming packets exceet The error-disable timeot applies to both the trusted packets across multiple The rate of the incomining packets from all the chart	upport for this command was introduced on the Catalyst 4500 series switch. Added support for interface monitoring. be configured with higher rates to reflect their aggregation. When the rate of the eds the user-configured rate, the interface is placed into an error-disabled state. but feature can be used to remove the port from the error-disabled state. The rate ed and nontrusted interfaces. Configure appropriate rates on trunks to handle the	

This example shows how to limit the rate of the 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	Command	Description
	show ip arp inspection	Displays the status of dynamic ARP inspection for a specific range of VLANs.

ip arp inspection log-buffer

To configure the parameters that are associated with the logging buffer, use the **ip arp inspection log-buffer** command. To disable the parameters, use the **no** form of this command.

ip arp inspection log-buffer {**entries** *number* | **logs** *number* **interval** *seconds*}

no ip arp inspection log-buffer {entries | logs}

Syntax Description	entries number	Number of entries from the logging buffer; the range is from 0 to 1024.
	logs number	Number of entries to be logged in an interval; the range is from 0 to 1024. A 0 value indicates that entries should not be logged out of this buffer.
	interval seconds	Logging rate; the range is from 0 to 86400 (1 day). A 0 value indicates an immediate log.
Defaults	When dynamic ARP	inspection is enabled, denied, or dropped, the ARP packets are logged.
	The number of entrie	es is set to 32.
	The number of loggi	ng 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	flow are registered b	cket of a given flow is logged immediately. The subsequent packets for the same ut are not logged immediately. Registering these packets is done in a log buffer that /LANs. 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)# ig Switch(config)# en Switch# show ip ar Total Log Buffer S	n commands, one per line. End with CNTL/Z. arp inspection log-buffer entries 45 d p inspection log Size : 45 stries per 1 seconds.

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

Command	Description	
arp access-list	Defines an ARP access list or adds clauses at the end of a predefined list.	
show ip arp inspection	Displays the status of dynamic ARP inspection for a specific range of VLANs.	

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. To make the interfaces untrusted, use the **no** form of this command.

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 this command:

```
Switch# show ip arp inspection interfaces fastEthernet 6/3
```

Interface	Trust State	Rate (pps)	Burst Interval
Fa6/3	Trusted	None	1
Switch#			

Related Commands	Command	Description
	show ip arp inspection	Displays the status of dynamic ARP inspection for a specific range of VLANs.

ip arp inspection validate

To perform specific checks for ARP inspection, use the **ip arp inspection validate** command. To disable checks, use the **no** form of this command.

ip arp inspection validate [src-mac] [dst-mac] [ip]

no ip arp inspection validate [src-mac] [dst-mac] [ip]

Syntax Description	src-mac	· •	nal) Checks the source MAC address in the Ethernet header against the sender's address in the ARP body. This checking is done against both ARP requests and uses.
		Note	When src-mac is enabled, packets with different MAC addresses are classified as invalid and are dropped.
	dst-mac		nal) Checks the destination MAC address in the Ethernet header against the MAC address in ARP body. This checking is done for ARP responses.
		Note	When dst-mac is enabled, the packets with different MAC addresses are classified as invalid and are dropped.
	ір	· •	nal) Checks the ARP body for invalid and unexpected IP addresses. Addresses e 0.0.0.0, 255.255.255.255, and all IP multicast addresses.
			ender IP addresses are checked in all ARP requests and responses and target IP uses are checked only in ARP responses.
Command Modes	Configuration		
Command History	Release	l	Nodification
	12.1(19)EW	Ś	Support for this command was introduced on the Catalyst 4500 series switch.
Usage Guidelines	command line. enables src and	Each co d dst ma	ecks, specify at least one of the keywords (src-mac , dst-mac , and ip) on the command overrides the configuration of the previous command. If a command ac validations, and a second command enables IP validation only, the src and dst sabled as a result of the second command.
	The no form o enabled, all the		mmand disables only the specified checks. If none of the check options are are disabled.

Examples	This exan	nple show how to e	nable the sour	ce MAC validatio	on:
	Switch(config)# ip arp inspe Switch(config)# end Switch# show ip arp inspecti Source Mac Validation : Destination Mac Validation : IP Address Validation :		ction vlan 1 : Enabled n : Disabled		
	Vlan	Configuration		ACL Match	Static ACL
	1 Vlan 	Enabled ACL Logging		ng 	
	1 Switch#	Deny	Deny		

Related Commands	Command	Description
	arp access-list	Defines an ARP access list or adds clauses at the end of a predefined list.
	show ip arp inspection	Displays the status of dynamic ARP inspection for a specific range of VLANs.

ip arp inspection vlan

To enable dynamic ARP inspection (DAI) on a per-VLAN basis, use the **ip arp inspection vlan** command. To disable DAI, use the **no** form of this command.

ip arp inspection vlan vlan-range

no ip arp inspection vlan vlan-range

Syntax Description	vlan-range	VLAN n	umber or rang	e; valid values are	e from 1 to 4094.
Defaults	ARP inspection	ı is disabled	on all VLANs		
Command Modes	Configuration				
Command History	Release	Modi	fication		
	12.1(19)EW	Supp	ort for this cor	nmand was introd	luced on the Catalyst 4500 series switch.
Usage Guidelines	they have not b	een created	or if they are p	orivate.	ay not function on the configured VLANs if
Examples	This example s Switch# confi Switch(config Switch(config Switch# show	gure termin)# ip arp i)# end	nal Inspection vl	an 1	
	Source Mac Va Destination M IP Address Va Vlan Conf	ac Validati	: Disable	đ	Static ACL
	1 Ena Vlan ACL	bled Logging	Active DHCP Loggi:	ng	
	 1 Den Switch#	 У	Deny		
	This example s	hows how to	o disable DAI o	on VLAN 1:	

Related Commands	Command	Description
	arp access-list	Defines an ARP access list or adds clauses at the end of a predefined list.
	show ip arp inspection	Displays the status of dynamic ARP inspection for a specific range of VLANs.

ip arp inspection vlan logging

To control the type of packets that are logged, use the **ip arp inspection vlan logging** command. To disable this logging control, use the **no** form of this command.

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	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.				
non	none	none Prevents all logging of packets permitted or denied by DHCP bindings.				
Defaults	All denied or dro	pped 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	configuration, the command to rese	nd dhcp-bindings keywords merge with each other. When you set an ACL match e DHCP bindings configuration is not disabled. You can use the no form of this t some of the logging criteria to their defaults. If you do not specify either option, al				
	the logging types	are reset to log on when the ARP packets are denied. The two options that are availab				

- 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

to you are as follows:

Examples This example shows how to configure an ARP inspection on VLAN 1 to add packets to a log on matching against the 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 DHCP Logging Vlan ACL Logging _____ _ _ _ _ -----1 Acl-Match Deny Switch#

Related Commands

Command	Description
arp access-list	Defines an ARP access list or adds clauses at the end of a predefined list.
show ip arp inspection	Displays the status of dynamic ARP inspection for a specific range of VLANs.

ip cef load-sharing algorithm

To configure the load-sharing hash function so that the source TCP/UDP port, the destination TCP/UDP port, or both ports 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 | destination dest} | original |
 tunnel | universal}

no ip cef load-sharing algorithm {include-ports {source | destination dest} | original | tunnel | universal}

Syntax Description	include-ports	Specifies the algorithm that includes the Layer 4 ports.		
	source source	Specifies the source port in the load-balancing hash functions.		
	destination dest	Specifies the destination port in the load-balancing hash. Uses the source and		
		destination in hash functions.		
	original	Specifies the original algorithm; not recommended.		
	tunnel	Specifies the algorithm for use in tunnel-only environments.		
	universal	Specifies the default Cisco IOS load-sharing algorithm.		
Defaults	Default load-sha	ing algorithm is disabled.		
 Note	This option does	not include the source or destination port in the load-balancing hash.		
Command Modes	Global configura	tion mode		
	6			
Command History	Release	Modification		
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.		
Usage Guidelines		rithm, tunnel algorithm, and universal algorithm are routed through the hardware. For		
	software-routed packets, the algorithms are handled by the software. The include-ports option does not			
	apply to the software-switched traffic.			
Examples		was how to configure the ID CEE load charing algorithm that includes Lover 4 parts.		
	This example sho	WS NOW TO COMPRETE THE IF CEF TOAT-SHALLING AIGOLIUM THAT MEDICES LAVEL 4 DOLLS.		
	-	bws how to configure the IP CEF load-sharing algorithm that includes Layer 4 ports:		
	-	ip cef load-sharing algorithm include-ports		

This example shows how to configure the IP CEF load-sharing algorithm that includes Layer 4 tunneling ports:

Switch(config)# ip cef load-sharing algorithm include-ports tunnel Switch(config)#

Related Commands

5	Command	Description	
	show ip cef vlan	Displays the IP CEF VLAN interface status and	•
		configuration information.	

ip device tracking maximum

To enable IP port security binding tracking on a Layer 2 port, use the **ip device tracking maximum** command. To disable IP port security on untrusted Layer 2 interfaces, use the **no** form of this command.

ip device tracking maximum {number}

no ip device tracking maximum {*number*}

Syntax Description		Specifies the number of bindings created in the IP device tracking table for a port, valid values are from 0 to 2048.
Defaults	This comman	nd has no default settings.
Command Modes	Interface con	figuration mode
Command History	Release	Modification
	12.2(37)SG	Support for this command was introduced on the Catalyst 4500 series switch.
Examples	This example	shows how to enable IP Port Security with IP-Mac filters on a Layer 2 access port:
	<pre>Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# ip device tracking Switch(config)# interface fastethernet 4/3 Switch(config-if)# switchport mode access Switch(config-if)# switchport access vlan 1 Switch(config-if)# ip device tracking maximum 5 Switch(config-if)# switchport port-security Switch(config-if)# switchport port-security maximum 5 Switch(config-if)# ip verify source tracking port-security Switch(config-if)# ip verify source tracking port-security Switch(config-if)# ip verify source tracking port-security</pre>	

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

Related Commands	Command	Description
	ip verify source	Enables IP source guard on untrusted Layer 2 interfaces.
	show ip verify source	Displays the IP source guard configuration and filters on a particular interface.

ip dhcp snooping

L

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 mode

Command HistoryReleaseModification12.1(12c)EWSupport 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	Command	Description
	ip dhcp snooping information option	Enables DHCP option 82 data insertion.
	ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
	ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
	ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
	show ip dhcp snooping	Displays the DHCP snooping configuration.
	show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

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	mac-address	Specifies a MAC address.	
	vlan vlan-#	Specifies a valid VLAN number.	
	ip-address	Specifies an IP address.	
	interface interfac	<i>ce</i> Specifies an interface type and number.	
	expiry seconds	Specifies the interval (in seconds) after which binding is no longer valid.	
Defaults	This command ha	s no default settings.	
Command Modes	Privileged EXEC	mode	
Command History	Release	Modification	
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.	
	12.2(25)EW	Support for the 10-Gigabit Ethernet interface 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 change and a write is initiated.		
Examples	This example shows how to generate a DHCP binding configuration on interface gigabitethernet1/1 ir VLAN 1 with an expiration time of 1000 seconds:		
Switch# ip dhcp sn Switch#	nooping binding 00	01.1234.1234 vlan 1 172.20.50.5 interface gil/1 expiry 1000	
Related Commands	Command	Description	

Related Commands	Command	Description
	ip dhcp snooping	Globally enables DHCP snooping.
	ip dhcp snooping information option	Enables DHCP option 82 data insertion.
	ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
	ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.

Command	Description
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

ip dhcp snooping database

To store the bindings that are generated by DHCP snooping, use the **ip dhcp snooping database** command. To either reset the timeout, reset the write-delay, or delete the agent specified by the URL, use the **no** form of this command.

ip dhcp snooping database {url | timeout seconds | write-delay seconds}

no ip dhcp snooping database {timeout | write-delay}

Syntax Description	url	Specifies the URL in one of the following forms:
		• tftp:// <host>/<filename></filename></host>
	• ftp:// <user>:<password>@<host>/<filename></filename></host></password></user>	
		• rcp:// <user>@<host>/<filename></filename></host></user>
		• nvram:/ <filename></filename>
		 bootflash:/<filename></filename>
	timeout seconds	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 an infinite duration.
	write-delay seconds	Specifies the duration for which the transfer should be delayed after a change to the binding database.
Command Modes	The write-delay va	alue is set to 300 seconds. ation mode
Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Usage Guidelines	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.	
Note	is recommended . creation of new file a large number of t	RAM and bootflash have limited storage capacity, using TFTP or network-based files If you use flash to store the database file, new updates (by the agent) result in the es (flash fills quickly). In addition, due to the nature of the filesystem used on the flash, files cause access to be considerably slowed. When a file is stored in a remote location in TFTP, an RPR/SSO standby supervisor engine can take over the binding list when a

switchover occurs.

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 dat Switch(config)# end Switch# show ip dhcp snooping databa Agent URL : tftp://10.1.1.1/directory Write delay Timer : 300 seconds Abort Timer : 300 seconds	se			
	Agent Running : Yes Delay Timer Expiry : Not Running Abort Timer Expiry : Not Running Last Succeded Time : None Last Failed Time : None Last Failed Reason : No failure recorded.				
	Media Failures : 0 Fa Switch#	ilea writes . 0			
	Related Commands	Command	Description		
	ip dhcp snooping	Globally enables DHCP snooping.			
	ip dhcp snooping binding	Sets up and generates a DHCP binding configuration to restore bindings across reboots.Enables DHCP option 82 data insertion.Enables DHCP snooping on a trusted VLAN.Enables DHCP snooping on a VLAN or a group of VLANs.Displays the DHCP snooping configuration.			
	ip dhcp snooping information option				
	ip dhcp snooping trust				
	ip dhcp snooping vlan				
	show ip dhcp snooping				
	show ip dhcp snooping binding	Displays the DHCP snooping binding entries.			

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 format remote-id {hostname | string {word}}

no ip dhcp snooping information option format remote-id {hostname | string {word}}

Syntax Description	format	Specifies the Option 82 information format.	
	remote-id	Specifies the remote ID for Option 82.	
	hostname	Specifies the user-configured hostname for the remote ID.	
	string word	Specifies the user defined string for the remote ID. The word string can be from 1 to 63 characters long with no spaces.	
Defaults	DHCP option 82	2 data insertion is enabled.	
Command Modes	Global configur	ation mode	
Command History	Release	Modification	
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.	
	12.2(40)SG	Added remote-id keyword to support Option 82 enhancement.	
Usage Guidelines Examples		is longer than 63 characters it is truncated to 63 characters in the Remote ID.	
Lingitus	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)#		
	This example shows how to configure the hostname as the Remote ID:		
	<pre>Switch(config)# ip dhcp snooping information option format remote-id hostname Switch(config)#</pre>		
	The following example shows how to enable DHCP Snooping on Vlan 500 through 555 and Opton 82 remote-id.		
Switch# configure Enter configuration Switch(config)# ig	on commands, one	per line. End with CNTL/Z.	

Catalyst 4500 Series Switch Cisco IOS Command Reference—Release 12.2(46)SG
```
Switch(config)# ip dhcp snooping vlan 500 555
Switch(config)# ip dhcp snooping information option format remote-id string switch123
Switch(config)# interface GigabitEthernet 5/1
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit rate 100
Switch(config-if)# ip dhcp snooping vlan 555 information option format-type circuit-id string customer-555
Switch(config-if)# interface FastEthernet 2/1
Switch(config-if)# ip dhcp snooping vlan 555 information option format-type circuit-id string customer-500
Switch(config)# interface FastEthernet 2/1
Switch(config)# end
```

Related Commands Comm

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
ip dhcp snooping binding	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
ip dhcp snooping vlan number information option format-type	Enables circuit-id (a sub-option of DHCP snooping option-82) on a VLAN.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

ip dhcp snooping information option allow-untrusted

To allow DHCP packets with option 82 data inserted to be received from a snooping untrusted port, use the **ip dhcp snooping information option allow-untrusted** command. To disallow receipt of these DHCP packets, use the **no** form of this command.

ip dhcp snooping information option allow-untrusted

no ip dhcp snooping information option allow-untrusted

Syntax Description	This command has n	no arguments or keywords.
--------------------	--------------------	---------------------------

Defaults DHCP packets with option 82 are not allowed on snooping untrusted ports.

Command Modes Global configuration mode

Command History	Release	Modification	
	12.2(25)EWA Support for this command was introduced on the Catalyst 4500 serie		

Examples This example shows how to allow DHCP packets with option 82 data inserted to be received from a snooping untrusted port:

Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# ip dhcp snooping information option allow-untrusted Switch(config)# end Switch#

Related Commands C

Related Commands	Command	Description
	ip dhcp snooping	Globally enables DHCP snooping.
	ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
	ip dhcp snooping information option	Enables DHCP option 82 data insertion.
	ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
	ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
	show ip dhcp snooping	Displays the DHCP snooping configuration.
	show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

• .•

ip dhcp snooping limit rate

To configure the number of the DHCP messages that an interface can receive per second, use the **ip dhcp snooping limit rate** command. To disable the 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	rate Numb	er of DHCP messages a	switch can receive per second.
Defaults	DHCP snooping 1	ate limiting is disabled.	
Command Modes	Interface configur	ration mode	
Command History	Release	Modification	
	12.1(12c)EW	Support for this comm	and was introduced on the Catalyst 4500 series switch.
Usage Guidelines	Typically, the rate limit applies to the untrusted interfaces. If you want to set up rate limiting for the trusted interfaces, note that the trusted interfaces aggregate all DHCP traffic in the switch, and you will need to adjust the rate limit of the interfaces to a higher value.		
Examples	This example sho	ws how to enable the D	HCP message rate limiting:
	Switch(config-if)# ip dhcp snooping limit rate 150 Switch(config)#		limit rate 150
	This example sho	ws how to disable the D	HCP message rate limiting:
	Switch(config)# no ip dhcp snooping limit rate Switch(config)#		ng limit rate
Related Commands	Command		Description
	ip dhcp snoopin	g	Globally enables DHCP snooping.
	ip dhcp snoopin	g information option	Enables DHCP option 82 data insertion.
	ip dhcp snoopin	g trust	Enables DHCP snooping on a trusted VLAN.
	ip dhcp snoopin	g vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
	show ip dhcp sn	ooping	Displays the DHCP snooping configuration.
	show ip dhcp sn	ooping binding	Displays the DHCP snooping binding entries.

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 mode

 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	Command	Description
	ip dhcp snooping	Globally enables DHCP snooping.
	ip dhcp snooping information option	Enables DHCP option 82 data insertion.
	ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
	ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
	show ip dhcp snooping	Displays the DHCP snooping configuration.
	show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

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 configura	ation mode	
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 global snooping and the VLAN snooping are enabled.		
Examples	-	ows how to enable DHCP snooping on a VLAN:	
	Switch(config) Switch(config)	# ip dhcp snooping vlan 10 #	
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:		ows how to disable DHCP snooping on a VLAN:	
		ows how to enable DHCP snooping on a group of VLANs:	
	Switch(config) Switch(config)	# ip dhcp snooping vlan 10 55 #	
	This example sh	ows how to disable DHCP snooping on a group of VLANs:	
	Switch(config) Switch(config)	# no ip dhcp snooping vlan 10 55 #	

Related

ted Commands	Command	Description
	ip dhcp snooping	Globally enables DHCP snooping.
	ip dhcp snooping information option	Enables DHCP option 82 data insertion.
	ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
	ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
	ip dhcp snooping vlan number information option format-type	Enables circuit-id (a sub-option of DHCP snooping option-82) on a VLAN.
	show ip dhcp snooping	Displays the DHCP snooping configuration.
	show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

ip dhcp snooping vlan number information option format-type

To enable circuit-id (a sub-option of DHCP snooping option-82) on a VLAN, use the **ip dhcp snooping vlan** *number* **information option format-type** command. To disable circuit-id on a VLAN, use the **no** form of this command.

ip dhcp snooping vlan number information option format-type circuit-id string string

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

Syntax Description	vlan numberSingle VLAN number or a range of VLANs; valid values are from 1 to 409		
	information	Specifies DHCP snooping information 82 data insertion.	
	option	Specifies DHCP snooping information option.	
	format-type	Specifies option-82 information format.	
	circuit-id	Specifies using the string as the circuit ID.	
	string string	Specifies a user-defined string for the circuit ID.	
Defaults	VLAN-mod-por	rt, if DHCP snooping option-82 is disabled.	
Command Modes	Interface config	uration mode	
Command History	Release Modification		
	12.2(40)SG	Support for this command was introduced on the Catalyst 4500 series switch.	
Usage Guidelines	The curcuit-id suboption of DHCP option-82 is supported only when DHCP snooping is globally enabled and on VLANs using DHCP option-82.		
Examples	The following example shows how to enable DHCP Snooping on Vlan 500 through 555 and Opton 82 circuit-id.		
<pre>Switch(config)# ig Switch(config)# ig Switch(config)# ig Switch(config)# im Switch(config-if)# Switch(config-if)# Switch(config-if)# Switch(config-if)#</pre>	on commands, one of dhcp snooping of dhcp snooping of dhcp snooping terface Gigabith ip dhcp snoopin ip dhcp snoopin ip dhcp snoopin ip dhcp snoopin ip dhcp snoopin interface Fasth ip dhcp snoopin	information option format remote-id string switch123 Ethernet 5/1 ng trust ng limit rate 100 ng vlan 555 information option format-type circuit-id string customer-555	

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

ip igmp filter

To control whether all hosts on a Layer 2 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	profile number	IGMP profile number to be applied; valid values are from 1 to 429496795.
Defaults	Profiles are not ap	plied.
Command Modes	Interface configura	ation mode
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	Command	Description
	ip igmp profile show ip igmp pro	Create an IGMP profile. Displays all configured IGMP profiles or a specified 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	number	Maximum number of IGMP groups that an interface can join; valid values are from 0 to 4294967294.	
Defaults	No maximum li	mit.	
Command Modes	Interface config	uration mode	
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 the ip igmp max-groups command only on Layer 2 physical interfaces; you cannot set the IGMP maximum groups for the routed ports, the switch virtual interfaces (SVIs), or the 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	n <i>profile number</i> IGMP profile number being configured; valid values are from 1 to 429			
Defaults	No profile created	1.		
Command Modes	Global configurat	ion mode		
	IGMP profile con	figuration		
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:			
	<pre>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)#</pre>			
Related Commands	Command	Description		
	ip igmp filter	Controls whether all hosts on a Layer 2 interface can join one or more IP multicast groups by applying an IGMP profile to the interface.		
	show ip igmp pr	ofile Displays all configured IGMP profiles or a specified IGMP profile.		

ip igmp query-interval

To configure the frequency that the switch sends the 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	seconds	Frequency, in seconds, at which the IGMP host-query messages are transmitted; valid values depend on the IGMP snooping mode. See the "Usage Guidelines" section for more information.	
Defaults	The query in	iterval is set to 60 seconds.	
Command Modes	Interface configuration mode		
Command History	Release	Modification	
-	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.	
Usage Guidelines	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. The designated switch for a LAN is the only switch that sends the 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.		
	1	are heard for the timeout period (controlled by the ip igmp query-timeout command), the nes the querier.	
<u>Note</u>	Changing th	e timeout period may severely impact multicast forwarding.	
Examples	This exampl host-query n	e shows how to change the frequency at which the designated switch sends the IGMP nessages:	

Switch(config-if)# ip igmp query-interval 120
Switch(config-if)#

Related Commands	Command	Description
	ip igmp querier-timeout (refer to Cisco IOS documentation)	Configures the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying.
	ip pim query-interval (refer to Cisco IOS documentation)	Configures the frequency of Protocol Independent Multicast (PIM) router query messages.
	show ip igmp groups (refer to Cisco IOS documentation)	Displays the multicast groups with receivers that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP), use the show ip igmp groups command in EXEC mode.

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 the topology change configurations.				
	flood	(Optional) Specifies to flood the spanning-tree table to the network when a topology change occurs. (Optional) Specifies the TCN query configurations.				
	query					
	count count	t (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 snoopin	g is enabled.				
Command Modes	Global configu	Global configuration mode				
	Interface config	guration mode				
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 ports, VLAN interfaces, or Layer 3 channels.					
	The ip igmp s r	nooping 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 s	This example shows how to disable IGMP snooping:				
	Switch(config Switch(config)# no ip igmp snooping)#				

This example shows how to enable the flooding of the spanning-tree table to the network after nine topology changes have occurred:

Switch(config)# ip igmp snooping tcn flood query count 9
Switch(config)#

This example shows how to disable the flooding of 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 Command

Command	Description
ip igmp snooping vlan immediate-leave	Enable IGMP immediate-leave processing.
ip igmp snooping vlan mrouter	Configures a Layer 2 interface as a multicast router interface for a VLAN.
ip igmp snooping vlan static	Configures a Layer 2 interface as a member of a group.

ip igmp snooping report-suppression

To enable report suppression, use the **ip igmp snooping report-suppression** command. To disable report suppression and forward the reports to the 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 keeping the second s	ceywords.
--	-----------

- **Defaults** IGMP snooping report-suppression is enabled.
- **Command Modes** Global configuration mode

 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 the IGMP reports are forwarded to the multicast devices.

If the command is enabled, report suppression is done by IGMP snooping.

Examples This exam

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#
```

Related Commands	Command	Description
	ip igmp snooping vlan immediate-leave	Enable IGMP immediate-leave processing.
	ip igmp snooping vlan mrouter	Configures a Layer 2 interface as a multicast router interface for a VLAN.
	ip igmp snooping vlan static	Configures a Layer 2 interface as a member of a group.

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 mode		
Command History	Release Modification		
-	12.1(8a)EW	Support for this comma	and was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended a	ddressing was added.
Examples	This example shows how to enable IGMP snooping on a VLAN:		
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	Command		Description
	ip igmp snoopi	ng vlan immediate-leave	Enable IGMP immediate-leave processing.
	ip igmp snoopi	ng vlan mrouter	Configures a Layer 2 interface as a multicast router interface for a VLAN.
	ip igmp snoopi	ng vlan static	Configures a Layer 2 interface as a member of a group.

interface for a VLAN.

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)EWSupport 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:			
	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:			
	Switch(config)# no ip igmp snooping vlan 200 explicit-tracking Switch(config)# end Switch# show ip igmp snooping vlan 200 include explicit tracking			
	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: 			
	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: 			
Related Commands	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: 			

Command	Description
ip igmp snooping vlan static	Configures a Layer 2 interface as a member of a group.
show ip igmp snooping membership	Displays host membership information.

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	vlan_num	Number of the	VLAN; valid values are from 1 to 4094.
-	immediate-leave	Enables imme	diate leave processing.
Defaults	Immediate leave p	rocessing is disabled.	
Command Modes	Global configuration mode		
Command History	Release Modification		
	12.1(8a)EW	Support for this com	mand 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-lea	ve feature is supporte	ed 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	Command		Description
	ip igmp snooping		Enable IGMP snooping.
	ip igmp snooping	vlan mrouter	Configures a Layer 2 interface as a multicast router interface for a VLAN.
	ip igmp snooping	vlan static	Configures a Layer 2 interface as a member of a group.

Command	Description
show ip igmp interface	Displays the information about the IGMP-interface status and configuration.
show mac-address-table multicast	Displays information about the multicast MAC address table.

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.

- noip igmp snooping vlan vlan-id mrouter {interface { fastethernet slot/port} | {gigabitethernet slot/port} | {tengigabitethernet slot/port} | {port-channel number} } | {learn {cgmp | pim-dvmrp}}

Syntax Description	vlan vlan-id	Specifies the VLAN ID number to use in the command; valid values are from 1 to 4094.
	interface	Specifies the next-hop interface to a multicast switch.
	fastethernet slot/port	Specifies the Fast Ethernet interface; number of the slot and port.
	gigabitethernet slot/port	Specifies the Gigabit Ethernet interface; number of the slot and port.
	tengigabitethernet <i>slot/port</i>	Specifies the 10-Gigabit Ethernet interface; number of the slot and port.
	port-channel number	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 mode

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(25)EW	Support for the 10-Gigabit Ethernet interface was introduced on the Catalyst 4500 series switch.

Usage Guidelines	You enter this command in VLAN interfac	ce 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 that you configure is	saved in NVRAM.		
	The static connections to multicast interfaces are supported only on switch interfaces.			
Examples	This example shows how to specify the ne	ext-hop interface to a 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 4 Switch(config-if)#	100 mrouter learn cgmp		
Related Commands	Command	Description		
	ip igmp snooping	Enable IGMP snooping.		
	ip igmp snooping vlan immediate-leave	Enable IGMP immediate-leave processing.		
	ip igmp snooping vlan static	Configures a Layer 2 interface as a member of a group.		
	show ip igmp snooping	Displays information on dynamically learned and manually configured VLAN switch interfaces.		
	show ip igmp snooping mrouter	Displays information on the dynamically learned and manually configured multicast switch interfaces.		

ip igmp snooping vlan static

To configure a 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*} | {**tengigabitethernet** *slot/port*} | {**port-channel** *number*}}
- **no ip igmp snooping vlan** *vlan_num static mac-address* {**interface** {**fastethernet** *slot/port*} | {**gigabitethernet** *slot/port*} | {**tengigabitethernet** *mod/interface-number*} | {**port-channel** *number*} }

Cuntou Decerintien		Number of the VLAN.
Syntax Description	vlan vlan_num	
	static mac-address	Group MAC address.
	interface	Specifies the next-hop interface to multicast switch.
	fastethernet slot/port	Specifies the Fast Ethernet interface; number of the slot and port.
	gigabitethernet slot/port	Specifies the Gigabit Ethernet interface; number of the slot and port.
	tengigabitethernet slot/por	<i>t</i> Specifies the 10-Gigabit Ethernet interface; number of the slot and port.
	port-channel number	Port-channel number; valid values are from 1 through 64.
Defaults	This command has no defau	t settings.
Command Modes	Global configuration mode	
Command History	Release Modificat	ion
	12.1(8a)EW Support f	or this command was introduced on the Catalyst 4500 series switch.
	12.2(25)EW Support f series swi	or the 10-Gigabit Ethernet interface was introduced on the Catalyst 4500 tch.
Examples	This example shows how to	configure a host statically on an interface:
		<pre>nooping vlan 4 static 0100.5e02.0203 interface fastethernet 5/11 rnet5/11 on group 0100.5e02.0203 vlan 4</pre>
		A
Related Commands	Command	Description
Related Commands	ip igmp snooping	Description Enable IGMP snooping. rediate-leave Enable IGMP immediate-leave processing.

Command	Description
ip igmp snooping vlan mrouter	Configures a Layer 2 interface as a multicast router interface for a VLAN.
show mac-address-table multicast	Displays information about the multicast MAC address table.

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 config	guration mode	
Command History	Release	Modification	
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.	
Usage Guidelines		only on subnets where hosts are intentionally prevented from communicating directly	
	to the switch on which they are connected.		
	ICMP redirect I	s disabled on interfaces where the local proxy ARP feature is enabled.	
Examples	This example sl	hows how to enable the local proxy ARP feature:	
	Switch(config- Switch(config-	-if)# ip local-proxy-arp -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

 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	Command	Description
	clear ip mfib fastdrop	Clears all the MFIB fast-drop entries.
	show ip mfib fastdrop	Displays all currently active fast-drop entries and shows whether fast drop is enabled.

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 statisti	ics is disabled.
	Inferred inform	ation is excluded.
Command Modes	Configuration	
Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switches.
	12.1(19)EW	Command enhanced to support infer fields.
Usage Guidelines	To use these cos	mmands, you need to install the Supervisor Engine IV and the NetFlow Service Card.
	IP address, dest	atistics feature captures a set of traffic statistics. These traffic statistics include the source ination IP address, Layer 4 port information, protocol, input and output identifiers, and formation that can be used for network analysis, planning, accounting, billing and S attacks.
	NetFlow switch	ing is supported on IP and IP-encapsulated traffic over all interface types.
	will purge the e	ip route-cache flow infer-fields command after the ip route-cache flow command, you xisting cache, and vice versa. This action is done to avoid having flows with and without n the cache simultaneously.
	For additional i Software Config	nformation on NetFlow switching, refer to the <i>Catalyst 4500 Series Switch Cisco IOS</i> guration Guide.
Note		mes additional memory and CPU resources compared to other switching modes. You he 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#



This command does not work on individual interfaces.

ip source binding

To add or delete a static IP source binding entry, use the **ip source binding** command. To delete the corresponding IP source binding entry, use the **no** form of this command.

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	ip-address	Binding IP address.
	mac-address	Binding MAC address.
	vlan vlan-id	VLAN number.
	interface interface-name	Binding interface.
Defaults	This command has no def	ault settings.
Command Modes	Global configuration mod	e
Command History	Release	Modification
-	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Usage Guidelines	The no form of this comm succeed, all required para Each static IP binding ent	ry is keyed by a MAC address and VLAN number. If the CLI contains an the existing binding entry will be updated with the new parameters; a separate
Examples	Switch# config terminal	to configure the static IP source binding: L rce binding 11.0.0.1 0000.000A.000B vlan 10 interface
Related Commands	Command	Description
	show ip source binding	Displays IP source bindings that are configured on the system.

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 mode

 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	Command	Description
	arp (refer to Cisco IOS documentation)	Enables Address Resolution Protocol (ARP) entries for static routing over the Switched Multimegabit Data Service (SMDS) network.
	show arp (refer to Cisco IOS documentation)	Displays ARP information.

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		loes not apply to Layer 3-switched (routed) packets. 00 series switch checks the validity of the following fields in the IPv4 header for all ackets:	
	 The version must be 4. The header length must be greater than or equal to 20 bytes. The total length must be greater than or equal to four times the header length and greater than Layer 2 packet size minus the Layer 2 encapsulation size. 		
	validation, the p	t fails the IP header validation, the packet is dropped. If you disable the header ackets with the invalid IP headers are bridged but are not routed even if routing was v4 access lists also are not applied to the IP headers.	
Examples	This example sh	ows how to disable the IP header validation for the Layer 2-switched IPv4 packets:	
	Switch# config Switch(config) Switch(config) Switch#	# no ip verify header vlan all	

ip verify source

To enable IP source guard on untrusted Layer 2 interfaces, use the **ip verify source** command. To disable IP source guard on untrusted Layer 2 interfaces, use the **no** form of this command.

ip verify source {vlan dhcp-snooping | tracking} [port-security]

no ip verify source {vlan dhcp-snooping | tracking} [port-security]

Syntax Description	vlan dhcp-snooping	Enables IP source guard on untrusted Layer 2 DHCP snooping interfaces.		
	tracking	Enables IP port security to learn static IP address learning on a port.		
	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 mode			
Command History Examples	Release Mo	odification		
	12.1(19)EW Su	pport for this command was introduced on the Catalyst 4500 series switch.		
	12.2(37)SG Ad	ded support for IP port security and tracking.		
	This example shows how to enable IP source guard on VLANs 10 through 20 on a per-port basis: Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# ip dhcp snooping Switch(config)# ip dhcp snooping vlan 10 20 Switch(config)# interface fastethernet6/1 Switch(config-if)# switchport trunk encapsulation dot1q Switch(config-if)# switchport trunk native vlan 10 Switch(config-if)# switchport trunk native vlan 10 Switch(config-if)# switchport trunk allowed vlan 11-20 Switch(config-if)# no ip dhcp snooping trust Switch(config-if)# ip verify source vlan dhcp-snooping			
	Switch(config-if)# Switch(config-if)# Switch(config-if)#	switchport trunk allowed vlan 11-20 no ip dhcp snooping trust ip verify source vlan dhcp-snooping		
	<pre>Switch(config-if)# Switch(config-if)# Switch(config-if)# Switch(config)# end</pre>	switchport trunk allowed vlan 11-20 no ip dhcp snooping trust ip verify source vlan dhcp-snooping 1		
	Switch(config-if)# Switch(config-if)# Switch(config-if)# Switch(config)# end Switch# show ip ver	switchport trunk allowed vlan 11-20 no ip dhcp snooping trust ip verify source vlan dhcp-snooping		

This example shows how to enable IP Port Security with IP-Mac filters on a Layer 2 access port:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface fastEthernet 4/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# ip verify source tracking port-security
```

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

Related	Commands	
---------	----------	--

Command	Description
ip device tracking maximum	Enables IP port security binding tracking on a Layer 2 port.
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
ip source binding	Adds or delete a static IP source binding entry.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip verify source	Displays the IP source guard configuration and filters on a particular interface.
show ip source binding	Displays IP source bindings that are configured on the system.
ip verify unicast source reachable-via

To enable and configure unicast RPF checks on a Supervisor Engine 6-E and Catalyst 4900M chassis IPv4 interface, use the **ip verify unicast source reachable-via** command. To disable unicast RPF, use the **no** form of this command.

ip verify unicast source reachable-via rx allow-default

no ip verify unicast source reachable-via

Syntax Description	rx	Verifies that the source address is reachable on the interface where the packet was received.
	allow-default	Verifies that the default route matches the source address.
Defaults	Disabled	
command Modes	Interface configu	uration mode
Command History	Release	Modification
	12.2(40)SG	Support for this command was introduced on the Catalyst 4500 with a Supervisor
Jsage Guidelines	In basic RX mod	Engine 6-E and the Catalyst 4900M chassis. le, unicast RPF ensures a source address must be reachable on the arrived interface. For
Jsage Guidelines <u>Note</u>	In basic RX modes and the source of the sour	Engine 6-E and the Catalyst 4900M chassis. le, unicast RPF ensures a source address must be reachable on the arrived interface. For rce must be reachable without load balancing.
	In basic RX mod example, the sour Unicast RPF is a end of a connect Do not use unica which means tha	Engine 6-E and the Catalyst 4900M chassis. le, unicast RPF ensures a source address must be reachable on the arrived interface. For rce must be reachable without load balancing.

Related Commands	Command	Description
	ip cef (refer to Cisco IOS documentation)	Enables Cisco Express Forwarding (CEF) on the switch.
	show running-config	Displays the current running configuration for a switch.

ipv6 mld snooping

To enable IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping globally or on the specified VLAN, use the **ipv6 mld snooping** command without keywords. To disable MLD snooping on a switch or the VLAN, use the **no** form of this command.

ipv6 mld snooping [vlan vlan-id]

no ipv6 mld snooping [vlan vlan-id]

Syntax Description	vlan vlan-id	(Optional) Enables or disables IPv6 MLD snooping on the specified VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.	
Defaults	MLD snooping is g	lobally disabled on the switch.	
	MLD snooping is enabled on all VLANs. However, MLD snooping must be globally enabled before VLAN snooping can take place.		
Command Modes	Global configuratio	on mode	
Command History	Release	Modification	
	12.2(40)SG	This command was introduced on the Catalyst 4500.	
Usage Guidelines	globally enable ML (enabled). VLAN c has been disabled.	ng is globally disabled, it is disabled on all the existing VLAN interfaces. When you LD snooping, it is enabled on all VLAN interfaces that are in the default state onfiguration overrides global configuration on interfaces on which MLD snooping s globally disabled, you cannot enable it on a VLAN. If MLD snooping is globally	
	enabled, you can disable it on individual VLANs. VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.		
Examples	This example shows how to globally enable MLD snooping: Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#ipv6 mld snooping Switch(config)#end Switch#		
	Switch# configure Enter configurati	on commands, one per line. End with CNTL/Z. • ipv6 mld snooping vlan 11	

Switch#

You can verify your settings by entering the show ipv6 mld snooping user EXEC command.

Related Commands

ds	Command	Description
	show ipv6 mld snooping	Displays IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping configuration of the switch or the VLAN.

ipv6 mld snooping last-listener-query-count

To configure IP version 6 (IPv6) Multicast Listener Discovery Mulitcast Address Specific Queries (MASQs) that will be sent before aging out a client, use the **ipv6 mld snooping last-listener-query-count** command. To reset the query count to the default settings, use the **no** form of this command.

ipv6 mld snooping [vlan vlan-id] last-listener-query-count integer_value

no ipv6 mld snooping [vlan vlan-id] last-listener-query-count

Syntax Description	vlan vlan-id	(Optional) Configure last-listener query count on the specified VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.
	integer_value	The range is 1 to 7.
Command Default	The default global	count is 2.
	The default VLAN	count is 0 (the global count is used).
Command Modes	Global configuratio	on mode
Command History	Release	Modification
Commanu History	norouoo	
oonnianu fiistory	12.2(40)SG	This command was introduced on the Catalyst 4500.
	In MLD snooping, multicast group. If query with a Multic Immediate Leave is the same port), the before an MLD clie	This command was introduced on the Catalyst 4500. the IPv6 multicast switch periodically sends out queries to hosts belonging to the a host wants to leave a multicast group, it can silently leave or it can respond to the cast Listener Done message (equivalent to an IGMP Leave message). When s not configured (it should not be configured if multiple clients for a group exist on configured last-listener query count determines the number of MASQs that are sent ent is aged out.
Usage Guidelines	In MLD snooping, multicast group. If query with a Multic Immediate Leave is the same port), the before an MLD clie When the last-lister When the VLAN co	This command was introduced on the Catalyst 4500. the IPv6 multicast switch periodically sends out queries to hosts belonging to the a host wants to leave a multicast group, it can silently leave or it can respond to the cast Listener Done message (equivalent to an IGMP Leave message). When s not configured (it should not be configured if multiple clients for a group exist on configured last-listener query count determines the number of MASQs that are sent

Examples This example shows how to globally set the last-listener query count: Switch#configure terminal

Enter configuration commands, one per line. End with CNTL/Z. Switch(config)**#ipv6 mld snooping last-listener-query-count 1** Switch(config)**#end** Switch#

This example shows how to set the last-listener query count for VLAN 10:

Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#ipv6 mld snooping vlan 10 last-listener-query-count 3 Switch(config)#end Switch#

You can verify your settings by entering the **show ipv6 mld snooping** [**vlan** *vlan-id*] user EXEC command.

Related Commands	Command	Description
	ipv6 mld snooping	Configures IP version 6 (IPv6) Multicast Listener
	last-listener-query-interval	Discovery (MLD) snooping last-listener query interval on the switch or on a VLAN.
	show ipv6 mld snooping	Displays IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping configuration of the switch or the VLAN.
	show ipv6 mld snooping querier	Displays IP version 6 (IPv6) MLD snooping querier-related information most recently received by the switch or the VLAN.

ipv6 mld snooping last-listener-query-interval

To configure IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping last-listener query interval on the switch or on a VLAN, use the **ipv6 mld snooping last-listener-query-interval** command. To reset the query time to the default settings, use the **no** form of this command.

ipv6 mld snooping [**vlan** *vlan-id*] **last-listener-query-interval** *integer_value*

no ipv6 mld snooping [vlan vlan-id] last-listener-query-interval

Syntax Description	vlan vlan-id(Optional) Configure last-listener query interval on the specifieVLAN ID range is 1 to 1001 and 1006 to 4094.	
	integer_value	Set the time period (in thousandths of a second) that a multicast switch must wait after issuing a MASQ before deleting a port from the multicast group. The range is 100 to 32,768. The default is 1000 (1 second),
Command Default	The default global	query interval (maximum response time) is 1000 (1 second).
	-	query interval (maximum response time) is 0 (the global count is used).
Command Modes	Global configuration	on mode
Command History	Release	Modification
-	12.2(40)SG	This command was introduced on the Catalyst 4500.
Usage Guidelines	-	ery-interval time is the maximum time that a multicast switch waits after issuing a Specific Query (MASQ) before deleting a port from the multicast group.
	to hosts belonging to of time, the switch	when the IPv6 multicast switch receives an MLD leave message, it sends out queries to the multicast group. If there are no responses from a port to a MASQ for a length deletes the port from the membership database of the multicast address. The last val is the maximum time that the switch waits before deleting a nonresponsive port group.
	When a VLAN quest set at 0, the global	ry interval is set, the global query interval is overridden. When the VLAN interval is value is used.
	VLAN numbers 10 in MLD snooping.	02 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used
Examples	This example show	s how to globally set the last-listener query interval to 2 seconds:
•	Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#ipv6 mld snooping last-listener-query-interval 2000 Switch(config)#end	

Switch#

This example shows how to set the last-listener query interval for VLAN 1 to 5.5 seconds:

Switch#configure terminal

```
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ipv6 mld snooping vlan 1 last-listener-query-interval 5500
Switch(config)#end
Switch#
```

You can verify your settings by entering the **show ipv6 MLD snooping** [**vlan** *vlan-id*] user EXEC command.

Related Commands	Command	Description
	ipv6 mld snooping	Configures IP version 6 (IPv6) Multicast Listener
	last-listener-query-count	Discovery Mulitcast Address Specific Queries (MASQs) that will be sent before aging out a client.
	show ipv6 mld snooping querier	Displays IP version 6 (IPv6) MLD snooping querier-related information most recently received by the switch or the VLAN.

ipv6 mld snooping listener-message-suppression

To enable IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping listener message suppression, use the **ipv6 mld snooping listener-message-suppression** command. To disable MLD snooping listener message suppression, use the **no** form of this command.

ipv6 mld snooping listener-message-suppression

no ipv6 mld snooping listener-message-suppression

Command Default The default is for MLD snooping listener message suppression to be disabled.

Command Modes Global configuration mode

Command History	Release	Modification
	12.2(40)SG	This command was introduced on the Catalyst 4500.

Usage Guidelines MLD snooping listener message suppression is equivalent to IGMP snooping report suppression. When it is enabled, received MLDv1 reports to a group are forwarded to IPv6 multicast switchs only once in every report-forward time. This prevents the forwarding of duplicate reports.

Examples This example shows how to enable MLD snooping listener message suppression:

Switch#configure terminal

```
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ipv6 mld snooping listener-message-suppression
Switch(config)#end
Switch#
```

This example shows how to disable MLD snooping listener message suppression:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ipv6 mld snooping listener-message-suppression
Switch(config)#end
Switch#
```

You can verify your settings by entering the **show ipv6 mld snooping** [**vlan** *vlan-id*] user EXEC command.

Related Commands	Command	Description
	ipv6 mld snooping	Enables IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping globally or on the specified VLAN.
	show ipv6 mld snooping	Displays IP version 6 (IPv6) MLD snooping configuration of the switch or the VLAN.

ipv6 mld snooping robustness-variable

To configure the number of IP version 6 (IPv6) Multicast Listener Discovery (MLD) queries that the switch sends before deleting a listener that does not respond, or to enter a VLAN ID to configure the number of queries per VLAN, use the **ipv6 mld snooping robustness-variable** command. To reset the variable to the default settings, use the **no** form of this command.

ipv6 mld snooping [vlan vlan-id] **robustness-variable** integer_value

no ipv6 mld snooping [vlan vlan-id] robustness-variable

Syntax Description	vlan vlan-id	(Optional) Configure the robustness variable on the specified VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.		
	integer_value	The range is 1 to 3.		
Command Default	The default global 1	robustness variable (number of queries before deleting a listener) is 2.		
		The default VLAN robustness variable (number of queries before aging out a multicast address) is 0, which means that the system uses the global robustness variable for aging out the listener.		
Command Modes	Global configuratio	on mode		
Command History	Release	Modification		
	12.2(40)SG	This command was introduced on the Catalyst 4500.		
Usage Guidelines	from a multicast gro number of MLDv1	ured by the number of MLDv1 queries sent with no response before a port is removed oup. A port is deleted when there are no MLDv1 reports received for the configured queries. The global value determines the number of queries that the switch waits stener that does not respond, and it applies to all VLANs that do not have a VLAN		
	The robustness value configured for a VLAN overrides the global value. If the VLAN robustness value is 0 (the default), the global value is used.			
	VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.			

Examples This example shows how to configure the global robustness variable so that the switch sends out three

queries before it deletes a listener port that does not respond: Switch#configure terminal

```
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ipv6 mld snooping robustness-variable 3
Switch(config)#end
Switch#
```

This example shows how to configure the robustness variable for VLAN 1. This value overrides the global configuration for the VLAN:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ipv6 mld snooping vlan 1 robustness-variable 1
Switch(config)#end
Switch#
```

You can verify your settings by entering the **show ipv6 MLD snooping** [**vlan** *vlan-id*] user EXEC command.

Related Commands	Command	Description
	ipv6 mld snooping	Configures IP version 6 (IPv6) Multicast Listener
	last-listener-query-count	Discovery Mulitcast Address Specific Queries (MASQs) that will be sent before aging out a client.
	show ipv6 mld snooping	Displays IP version 6 (IPv6) MLD snooping configuration of the switch or the VLAN.

ipv6 mld snooping tcn

To configure IP version 6 (IPv6) Multicast Listener Discovery (MLD) Topology Change Notifications (TCNs), use the **ipv6 mld snooping tcn** commands. To reset the default settings, use the **no** form of the commands.

ipv6 mld snooping tcn {**flood query count** *integer_value* | **query solicit**}

no ipv6 mld snooping tcn {flood query count *integer_value* | **query solicit**}

Syntax Description	flood query count integer_value	Set the flood query count, which is the number of queries that are sent before forwarding multicast data to only those ports requesting it. The range is 1 to 10.	
	query solicit	Enable soliciting of TCN queries.	
Command Default	TCN query soliciting i When enabled, the def	s disabled. ault flood query count is 2.	
Command Modes	Global configuration mode		
Command History	Release	Modification	
	12.2(25)SG	This command was introduced on the Catalyst 4500.	
Examples	This example shows how to enable TCN query soliciting: Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#ipv6 mld snooping tcn query solicit. Switch(config)#end Switch#		
	This example shows he	ow to set the flood query count to 5:	
	Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#ipv6 mld snooping tcn flood query count 5. Switch(config)#end Switch#		
	You can verify your se command.	ttings by entering the show ipv6 MLD snooping [vlan <i>vlan-id</i>] user EXEC	
Related Commands	Command	Description	
	show ipv6 mld snoop	Displays IP version 6 (IPv6) MLD snooping configuration of the switch or the VLAN.	

ipv6 mld snooping vlan

To configure IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping parameters on the VLAN interface, use the **ipv6 mld snooping vlan** command. To reset the parameters to the default settings, use the **no** form of this command.

no ipv6 mld snooping vlan *vlan-id* [**immediate-leave** | **mrouter interface** *interface-id* | **static** *ip-address* **interface** *interface-id*]

Syntax Description	vlan vlan-id	Specify a VLAN number. The range is 1 to 1001 and 1006 to 4094.
	immediate-leave	(Optional) Enable MLD Immediate-Leave processing on a VLAN
		interface. Use the no form of the command to disable the Immediate
		Leave feature on the interface.
	mrouter interface	(Optional) Configure a multicast switch port. The no form of the command removes the configuration.
	static ipv6-multicast-address	(Optional) Configure a multicast group with the specified IPv6 multicast address.
	interface interface-id	Add a Layer 2 port to the group. The mrouter or static interface can be a physical port or a port-channel interface ranging from 1 to 48.
Command Default	MLD snooping Immediate-Le	
Command Default	By default, there are no static	IPv6 multicast groups.
Command Default		IPv6 multicast groups.
	By default, there are no static	IPv6 multicast groups.
Command Default Command Modes Command History	By default, there are no static By default, there are no multic Global configuration mode	IPv6 multicast groups.
Command Modes	By default, there are no static By default, there are no multic Global configuration mode Release Mod	IPv6 multicast groups. cast switch ports.
Command Modes	By default, there are no static By default, there are no multic Global configuration mode Release Mod 12.2(40)SG This	IPv6 multicast groups. cast switch ports. dification s command was introduced on the Catalyst 4500. Immediate-Leave feature when there is only one receiver on every port in
Command Modes Command History	By default, there are no static By default, there are no multic Global configuration mode $\hline \hline \frac{\text{Release}}{12.2(40)\text{SG}} \hline \text{This}$ You should only configure the the VLAN. The configuration	IPv6 multicast groups. cast switch ports. dification s command was introduced on the Catalyst 4500. Immediate-Leave feature when there is only one receiver on every port in
Command Modes Command History	By default, there are no static By default, there are no multic Global configuration mode Release Mode 12.2(40)SG This You should only configure the the VLAN. The configuration The static keyword is used for	IPv6 multicast groups. cast switch ports. dification s command was introduced on the Catalyst 4500. Immediate-Leave feature when there is only one receiver on every port in is saved in NVRAM.

ipv6 mld snooping vlan *vlan-id* [**immediate-leave** | **mrouter interface** *interface-id* | **static** *ipv6-multicast-address* **interface** *interface-id*]

Examples This example shows how to enable MLD Immediate-Leave processing on VLAN 1: Switch#configure terminal

```
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ipv6 mld snooping vlan 1 immediate-leave
Switch(config)#end
Switch#
```

This example shows how to disable MLD Immediate-Leave processing on VLAN 1:

Switch#configure terminal

```
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ipv6 mld snooping vlan 1 immediate-leave
Switch(config)#end
Switch#
```

This example shows how to configure a port as a multicast switch port:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ipv6 mld snooping vlan 1 mrouter interface gigabitethernet1/0/2
Switch(config)#end
Switch#
```

This example shows how to configure a static multicast group:

```
Switch#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ipv6 mld snooping vlan 2 static FF12::34 interface gigabitethernet1/0/2
Switch(config)#end
Switch#
```

You can verify your settings by entering the **show ipv6 mld snooping vlan** *vlan-id* user EXEC command.

Related Commands	Command	Description
	ipv6 mld snooping	Enables IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping globally or on the specified VLAN.
	show ipv6 mld snooping	Displays IP version 6 (IPv6) MLD snooping configuration of the switch or the VLAN.

issu abortversion

To cancel the ISSU upgrade or the downgrade process in progress and to restore the Catalyst 4500 series switch to its state before the start of the process, use the **issue abortversion** command.

issu abortversion active-slot [active-image-new]

Syntax Description	active-slot	Specifies the slot number for the current standby supervisor engine.		
	active-image-new	(Optional) Name of the new image present in the current standby supervisor engine.		
Defaults	There are no default settings.			
Command Modes	Privileged EXEC mod	le		
Command History	Release	Modification		
	12.2(31)SGA	This command was introduced on the Catalyst 4500 series switch.		
Usage Guidelines	You can use the issu abortversion command at any time to stop the ISSU process. To complete the process enter the issu commitversion command. Before any action is taken, a check ensures that both supervisor engines are either in the run version (RV) or load version (LV) state. When the issu abortversion command is entered before the issu runversion command, the standby supervisor engine is reset and reloaded with the old image. When the issu abortversion command is entered after the issu runversion command, a change takes place and the new standby supervisor engine is reset and reloaded with the old image.			
Examples	This example shows h	now you can reset and reload the standby supervisor engine:		
Examples	This example shows h Switch# issu abortv Switch#			
	Switch# issu abortv			
Examples Related Commands	Switch# issu abortv Switch#	ersion 2		
	Switch# issu abortvo Switch#	Description Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically stopped during the		

Command	Description
issu runversion	Forces a change from the active supervisor engine to the standby supervisor engine and causes the newly active supervisor engine to run the new image specified.
show issu state	Displays the ISSU state and current booted image name during the ISSU process.

issu acceptversion

To halt the rollback timer and to ensure that the new Cisco IOS software image is not automatically stopped during the ISSU process, use the **issu acceptversion** command.

issu acceptversion active-slot [active-image-new]

Syntax Description	active-slot	Specifies the slot number for the currently active supervisor engine.			
	active-image-new	(Optional) Name of the new image on the current lyactive supervisor engine.			
Defaults	Rollback timer resets	Rollback timer resets automatically 45 minutes after you issue the issu runversion command.			
Command Modes	Privileged EXEC mode				
Command History	Release	Modification			
	12.2(31)SGA	This command was introduced on the Catalyst 4500 series switch.			
	If the issu acceptvers command is entered, t	ion command is not entered within 45 minutes from the time the issu runversion he entire ISSU process is automatically rolled back to the previous version of the			
Usage Guidelines	After you are satisfied with the new image and have confirmed the new supervisor engine is reachable by both the console and the network, enter the issu acceptversion command to halt the rollback timer. If the issu acceptversion command is not entered within 45 minutes from the time the issu runversion command is entered, the entire ISSU process is automatically rolled back to the previous version of the software. The rollback timer starts immediately after you issue the issu runversion command.				
	is automatically extended extension time or the	xpires before the standby supervisor engine goes to a hot standby state, the timer ded by up to 15 minutes. If the standby state goes to a hot-standby state within this 15 minute extension expires, the switch aborts the ISSU process. A warning your intervention is displayed every 1 minute of the timer extension.			
		s set to a long period of time, such as the default of 45 minutes, and the standby s into the hot standby state in 7 minutes, you have 38 minutes (45 minus 7) to roll			
	Use the issu set rollba	ack-timer to configure the rollback timer.			
Examples	This example shows h	ow to halt the rollback timer and allow the ISSU process to continue:			
	Switch# issu accept Switch#	version 2			

Command	Description
issu abortversion	Cancels the ISSU upgrade or the downgrade process in progress and restores the switch to its state before the start of the process.
issu commitversion	Loads the new Cisco IOS software image into the new standby supervisor engine.
issu loadversion	Starts the ISSU process.
issu runversion	Forces a change from the active supervisor engine to the standby supervisor engine and causes the newly active supervisor engine to run the new image specified.
issu set rollback-timer	Configures the In Service Software Upgrade (ISSU) rollback timer value.
show issu state	Displays the ISSU state and current booted image name during the ISSU process.
	issu abortversion issu commitversion issu loadversion issu runversion issu set rollback-timer

issu commitversion

To load the new Cisco IOS software image into the new standby supervisor engine, use the **issu commitversion** command.

issu commitversion *standby-slot standby-image-new*

Syntax Description	standby-slot	Specifies the slot number for the currently active supervisor engine.
	active-image-new	(Optional) Name of the new image on the currently active supervisor engine.
Defaults	Enabled by default.	
Command Modes	Privileged EXEC mod	le
Command History	Release	Modification
	12.2(31)SGA	This command was introduced on the Catalyst 4500 series switch.
Usage Guidelines	software image in its	ion command verifies that the standby supervisor engine has the new Cisco IOS file system and that both supervisor engines are in the run version (RV) state. If net, the following actions take place:
	• The standby super	rvisor engine is reset and booted with the new version of Cisco IOS software.
	• •	rvisor engine moves into the Stateful Switchover (SSO) mode and is fully stateful applications with which the standby supervisor engine is compatible.
	• The supervisor en	ngines are moved into final state, which is the same as initial state.
	-	mitversion command completes the In Service Software Upgrade (ISSU) process. e stopped or reverted to its original state without starting a new ISSU process.
	equivalent to entering issu commitversion c	mitversion command without entering the issu acceptversion command is both the issu acceptversion and the issu commitversion commands. Use the command if you do not intend to run in the current state for an extended period of with the new software version.
Examples	This example shows h the new Cisco IOS so	now you can configure the standby supervisor engine to be reset and reloaded with ftware version:
	Switch# issu commit	

Related Commands	Command	Description
	issu acceptversion	Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically stopped during the ISSU process.
	issu commitversion	Loads the new Cisco IOS software image into the new standby supervisor engine.
	issu loadversion	Starts the ISSU process.
	issu runversion	Forces a change from the active supervisor engine to the standby supervisor engine and causes the newly active supervisor engine to run the new image specified.
	show issu state	Displays the ISSU state and current booted image name during the ISSU process.

issu loadversion

To start the ISSU process, use the issu loadversion command.

issu loadversion active-slot active-image-new standby-slot standby-image-new [force]

	active-slot	Specifies the slot number for the currently active supervisor engine.		
Syntax Description		Specifies the name of the new image on the currently active supervisor engine.		
	active-image-new	Specifies the standby slot on the networking device.		
	standby-slot			
	standby-image-new	Specifies the name of the new image on the standby supervisor engine.		
	force	(Optional) Overrides the automatic rollback when the new Cisco IOS software version is detected to be incompatible.		
Defaults	This command has no default settings.			
Command Modes	Privileged EXEC mod	de		
Command History	Release	Modification		
	12.2(31)SGA	This command was introduced on the Catalyst 4500 series switch.		
	new Cisco IOS softwa ISSU capable, ISSU c	command causes the standby supervisor engine to be reset and booted with the are image specified by the command. If both the old image and the new image are compatible, and have no configuration mismatches, the standby supervisor engine witchover (SSO) mode, and both supervisor engines move into the load version.		
	new Cisco IOS softwa ISSU capable, ISSU c moves into Stateful S (LV) state. It will take several set	are image specified by the command. If both the old image and the new image are		
Usage Guidelines Examples	new Cisco IOS softwa ISSU capable, ISSU c moves into Stateful S (LV) state. It will take several sec load onto the standby	are image specified by the command. If both the old image and the new image are compatible, and have no configuration mismatches, the standby supervisor engine witchover (SSO) mode, and both supervisor engines move into the load version conds after the issu loadversion command is entered for Cisco IOS software to		
	new Cisco IOS softwa ISSU capable, ISSU c moves into Stateful S (LV) state. It will take several sec load onto the standby This example shows h	are image specified by the command. If both the old image and the new image are compatible, and have no configuration mismatches, the standby supervisor engine witchover (SSO) mode, and both supervisor engines move into the load version conds after the issu loadversion command is entered for Cisco IOS software to supervisor engine and the standby supervisor engine to transition to SSO mode.		
	new Cisco IOS softwa ISSU capable, ISSU c moves into Stateful S (LV) state. It will take several sec load onto the standby This example shows h Switch# issu loadve	are image specified by the command. If both the old image and the new image are compatible, and have no configuration mismatches, the standby supervisor engine witchover (SSO) mode, and both supervisor engines move into the load version conds after the issu loadversion command is entered for Cisco IOS software to supervisor engine and the standby supervisor engine to transition to SSO mode.		
Examples	new Cisco IOS softwa ISSU capable, ISSU c moves into Stateful S (LV) state. It will take several sec load onto the standby This example shows h Switch# issu loadve Switch#	are image specified by the command. If both the old image and the new image are compatible, and have no configuration mismatches, the standby supervisor engine witchover (SSO) mode, and both supervisor engines move into the load version conds after the issu loadversion command is entered for Cisco IOS software to supervisor engine and the standby supervisor engine to transition to SSO mode. how to initiate the ISSU process: prsion 1 bootflash:new-image 2 slavebootflash:new-image		

Command	Description
issu commitversion	Loads the new Cisco IOS software image into the new standby supervisor engine.
issu runversion	Forces a change from the active supervisor engine to the standby supervisor engine and causes the newly active supervisor engine to run the new image specified.
show issu state	Displays the ISSU state and current booted image name during the ISSU process.

issu runversion

To force a change from the active supervisor engine to the standby supervisor engine and to cause the newly active supervisor engine to run the new image specified in the **issu loadversion** command, use the **issu runversion** command.

issu runversion standby-slot [standby-image-new]

Syntax Description	standby-slot	Specifies the standby slot on the networking device.	
	standby-image-new	Specifies the name of the new image on the standby supervisor engine.	
Defaults	This command has no	default settings.	
Command Modes	Privileged EXEC mode		
Command History	Release	Modification	
	12.2(31)SGA	This command was introduced on the Catalyst 4500 series switch.	
Usage Guidelines	The issu runversion command changes the currently active-supervisor engine to standby-supervisor engine and the real standby-supervisor engine is booted with the old image version following and resets the switch. As soon as the standby-supervisor engine moves into the standby state, the rollback timer is started.		
Examples	This example shows how to force a change of the active-supervisor engine to standby-supervisor engine switch# issu runversion 2 Switch#		
Related Commands	Command	Description	
Related Commands	Command issu abortversion	Description Cancels the ISSU upgrade or the downgrade process in progress and restores the switch to its state before the start of the process.	
Related Commands		Cancels the ISSU upgrade or the downgrade process in progress and restores the switch to its state before the start	
Related Commands	issu abortversion	Cancels the ISSU upgrade or the downgrade process in progress and restores the switch to its state before the start of the process. Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically stopped during the	
Related Commands	issu abortversion	Cancels the ISSU upgrade or the downgrade process in progress and restores the switch to its state before the start of the process. Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically stopped during the ISSU process. Loads the new Cisco IOS software image into the new	

issu set rollback-timer

To configure the In Service Software Upgrade (ISSU) rollback timer value, use the **issu set rollback-timer** command.

issu set rollback-timer seconds

Syntax Description	seconds	Specfies the rollback timer value, in seconds. The valid timer value range i from 0 to 7200 seconds (2 hours). A value of 0 seconds disables the rollback timer.	
Defaults	Rollback timer value	e is 2700 seconds.	
Command Modes	Global configuration	mode	
Command History	Release	Modification	
	12.2(31)SGA	This command was introduced on the Catalyst 4500 series switch.	
Usage Guidelines Examples	this command when	Iback-timer command to configure the rollback timer value. You can only enable the supervisor engines are in the init state. how you can set the rollback timer value to 3600 seconds, or 1 hour:	
·	Switch# configure terminal Switch(config)# issu set rollback-timer 3600 Switch(config)# end Switch#		
Related Commands	Command	Description	
	issu acceptversion	Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically stopped during the ISSU process.	
	issu set rollback-tii	mer Configures the In Service Software Upgrade (ISSU) rollback timer value.	

l2protocol-tunnel

To enable protocol tunneling on an interface, use the **l2protocol-tunnel** command. You can enable tunneling for the Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunking Protocol (VTP) packets. To disable tunneling on the interface, use the **no** form of this command.

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 that	no Layer 2 protocol packets are tunneled.
Command Modes	Interface configuration mode	
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 Layer 2 protocol MAC address.	
		ver 2 protocol tunneling for CDP, STP, and VTP individually or for all three protocols
Examples	-	ys how to enable protocol tunneling for the CDP packets: # 12protocol-tunnel cdp #
Related Commands	Command	Description
	l2protocol-tunnel	cos Configures the class of service (CoS) value for all tunneled

Command	Description
12protocol-tunnel drop-threshold	Sets a drop threshold for the maximum rate of Layer 2 protocol packets per second to be received before an interface drops packets.
12protocol-tunnel shutdown-threshold	Configures the protocol tunneling encapsulation rate.

l2protocol-tunnel cos

To configure the class of service (CoS) value for all tunneled Layer 2 protocol packets, use the **l2protocol-tunnel cos** command. To return to the default value of zero, use the **no** form of this command.

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		oS value that is configured for data on the interface. If no CoS value is 5 for all tunneled Layer 2 protocol packets.		
Command Modes	Global configuration mode			
Command History	Release	Modification		
	12.2(18)EW	This command was first introduced on the Catalyst 4500 series switch.		
Usage Guidelines	When enabled, the tunnel The value is saved in NVI	ed Layer 2 protocol packets use this CoS value. RAM.		
Examples		to configure a Layer 2 protocol tunnel CoS value of 7:		
	Switch(config)# 12proto Switch(config)#	ocol-tunnel cos 7		
Related Commands	Command	Description		
	l2protocol-tunnel	Enables protocol tunneling on an interface.		
	12protocol-tunnel drop-1	Chreshold Sets a drop threshold for the maximum rate of Layer 2 protocol packets per second to be received before an interface drops packets.		
	l2protocol-tunnel shutde	wn-threshold Configures the protocol tunneling encapsulation rate.		

l2protocol-tunnel drop-threshold

To set a drop threshold for the maximum rate of Layer 2 protocol packets per second to be received before an interface drops packets, use the **I2protocol-tunnel drop-threshold** command. You can set the drop threshold for the Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunking Protocol (VTP) packets. To disable the drop threshold on the interface, use the **no** form of this command.

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.					
	value	<i>value</i> Specifies a threshold in packets per second to be received for encapsulation before the interface shuts down, or specifies 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 the Layer 2 protocol packets.				
Command Modes	Interface co	nfiguration mode				
Command History	Release	Modification				
	12.2(18)EW	V Support for this command was introduced on the Catalyst 4500 series switch.				
Usage Guidelines	The l2proto that are rece keyword, th shutdown th	Support for this command was introduced on the Catalyst 4500 series switch. col-tunnel drop-threshold command controls the number of protocol packets per second eived on an interface before it drops packets. When no protocol option is specified with a e threshold is applied to each of the tunneled Layer 2 protocol types. If you also set a ureshold on the interface, the drop-threshold value must be less than or equal to the mreshold value.				
Usage Guidelines	The l2proto that are rece keyword, th shutdown th shutdown-th When the du	bcol-tunnel drop-threshold command controls the number of protocol packets per second eived on an interface before it drops packets. When no protocol option is specified with a e threshold is applied to each of the tunneled Layer 2 protocol types. If you also set a ureshold on the interface, the drop-threshold value must be less than or equal to the				
Usage Guidelines Examples	The l2proto that are rece keyword, th shutdown th shutdown-th When the du which they	col-tunnel drop-threshold command controls the number of protocol packets per second eived on an interface before it drops packets. When no protocol option is specified with a e threshold is applied to each of the tunneled Layer 2 protocol types. If you also set a preshold on the interface, the drop-threshold value must be less than or equal to the preshold value. The protocol packets until the rate at the protocol packets until the packets until				

Related Commands Command

ands	Command	Description
	l2protocol-tunnel	Enables protocol tunneling on an interface.
	12protocol-tunnel cos	Configures the class of service (CoS) value for all tunneled Layer 2 protocol packets.
	l2protocol-tunnel shutdown-threshold	Configures the protocol tunneling encapsulation rate.

I

l2protocol-tunnel shutdown-threshold

To configure the protocol tunneling encapsulation rate, use the **I2protocol-tunnel shutdown-threshold** command. You can set the encapsulation rate for the Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunking Protocol (VTP) packets. To disable the encapsulation rate on the interface, use the **no** form of this command.

l2protocol-tunnel shutdown-threshold [cdp | stp | vtp] value

no l2protocol-tunnel shutdown-threshold [cdp | stp | vtp] value

Syntax Description	cdp (Op	ptional) Specifies a shutdown threshold for CDP.				
	stp (Op	ptional) Specifies a shutdown threshold for STP.				
	vtp (Op	(Optional) Specifies a shutdown threshold for VTP.				
	1					
Defaults	The default is no	shutdown threshold for the number of Layer 2 protocol packets.				
Command Modes	Interface configur	ration mode				
Command History	Release	Modification				
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.				
Usage Guidelines	second that are reacted the keyword, the	tunnel shutdown-threshold command controls the number of protocol packets per acceived on an interface before it shuts down. When no protocol option is specified with threshold is applied to each of the tunneled Layer 2 protocol types. If you also set a the interface, the shutdown-threshold value must be greater than or equal to the alue.				
	entering the errd i error-disabled sta error recovery fea	wn threshold is reached, the interface is error disabled. If you enable error recovery by isable recovery cause l2ptguard command, the interface is brought out of the atte and allowed to retry the operation again when all the causes have timed out. If the ature generation is not enabled for l2ptguard , the interface stays in the error-disabled ter the shutdown and no shutdown commands.				
Examples	This example sho	ows how to configure the maximum rate:				
	Switch(config-i: Switch(config-i:	f)# 12protocol-tunnel shutdown-threshold cdp 50 f)#				

Related Commands

Command	Description
l2protocol-tunnel	Enables protocol tunneling on an interface.
l2protocol-tunnel cos	Configures the class of service (CoS) value for all tunneled Layer 2 protocol packets.
l2protocol-tunnel drop-threshold	Sets a drop threshold for the maximum rate of Layer 2 protocol packets per second to be received before an interface drops packets.

lacp port-priority

To set the LACP priority for the 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 config	uration mode		
Command History	Release	Modification		
	12.1(13)EW	This command w	as introduced on the Catalyst 4500 series switches.	
Usage Guidelines	This command i	s not supported on t	he systems that are configured with a Supervisor Engine I.	
	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.			
	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.			
	When setting th	e priority, the higher	numbers indicate lower priorities.	
Examples	-	-	priority for the interface:	
	Switch(config- Switch(config-	if)# lacp port-pri if)#	lority 23748	
Related Commands	Command		Description	
	channel-group		Assigns and configure an EtherChannel interface to an EtherChannel group.	
	channel-protoc	col	Enables LACP or PAgP on an interface.	
	lacp system-pr	iority	Sets the priority of the system for LACP.	
	show lacp		Displays LACP information.	

lacp system-priority

To set the priority of the system for LACP, use the lacp system-priority command.

lacp system-priority priority

Syntax Description	priority	Priority of the system; valid values are from 1 to 65535.
Defaults	Priority is set to	68.
Command Modes	Global configura	1 mode
Command History	Release	Aodification
	12.1(13)EW	This command was introduced on the Catalyst 4500 series switches.
Usage Guidelines	This command is	t supported on systems that are configured with a Supervisor Engine I.
	You must assign each switch that is running LACP a system priority that can be or by entering the lacp system-priority command. The system priority is used address to form the system ID and is also used during negotiation with other system.	
		and is a global configuration command, the <i>priority</i> value is supported on port <i>P</i> -enabled physical interfaces.
When setting the priority, the higher numbers indicate lower priorities.		ority, tthe higher numbers indicate lower priorities.
	You can also enter the lacp system-priority command in interface configuration mode. After the command, the system defaults to global configuration mode.	
Examples	This example sho	how to set the system priority:
	Switch(config)# lacp system-priority 23748 Switch(config)#	
Related Commands	Command	Description
	channel-group	Assigns and configure an EtherChannel interface to an EtherChannel group.
	channel-protoco	Enables LACP or PAgP on an interface.
	lacp system-pri	
	show lacp	Displays LACP information.

logging event link-status global (global configuration)

To change the default switch-wide global link-status event messaging settings, use the **logging event link-status global** command. Use the **no** form of this command to disable the link-status event messaging.

logging event link-status global

no logging event link-status global

- **Syntax Description** This command has no arguments or keywords.
- **Defaults** The global link-status messaging is disabled.
- **Command Modes** Global configuration mode

Command History	Release	Modification	
	12.2(25)SG	Support for this command was introduced on the Catalyst 4500 series switch.	

Usage Guidelines If link-status logging event is not configured at the interface level, this global link-status setting takes effect for each interface.

Examples This example shows how to globally enable link status message on each interface: Switch# config terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# logging event link-status global Switch(config)# end Switch#

Related Commands	Command	Description	
	logging event link-status (interface configuration)	Enables the link-status event messaging on an interface.	

logging event link-status (interface configuration)

logging event link-status use-global command to apply the global link-status setting. logging event link-status no logging event link-status logging event link-status use-global Defaults Global link-status messaging is enabled. **Command Modes** Interface configuration mode **Command History** Release Modification 12.2(25)SG Support for this command was introduced on the Catalyst 4500 series switch. **Usage Guidelines** To enable system logging of interface state-change events on a specific interface, enter the logging event link-status command in interface configuration mode. To enable system logging of interface state-change events on all interfaces in the system, enter the logging event link-status global command in global configuration mode. All interfaces without the state change event configuration use the global setting. Examples This example shows how to enable logging event state-change events on interface gi11/1: Switch# config terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config) # interface gi11/1 Switch(config-if) # logging event link-status Switch(config-if) # end Switch# This example shows how to turn off logging event link status regardless of the global setting: Switch# config terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config) # interface gi11/1 Switch(config-if) # no logging event link-status Switch(config-if)# end Switch#

To enable the link-status event messaging on an interface, use the logging event link-status command.

Use the no form of this command to disable link-status event messaging. Use the

L

This example shows how to enable the global event link-status setting on interface gi11/1:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gill/1
Switch(config-if)# logging event link-status use-global
Switch(config-if)# end
Switch#
```

Related Commands Command

Command	Description
logging event link-status global (global	Changes the default switch-wide global link-status event
configuration)	messaging settings.
logging event trunk-status global (global configuration)

To enable the trunk-status event messaging globally, use the **logging event trunk-status global** command. Use the **no** form of this command to disable trunk-status event messaging.

logging event trunk-status global

no logging event trunk-status global

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

Defaults	Global trunk-status	messaging is disabled.
----------	---------------------	------------------------

Command Modes Global configuration mode

Command HistoryReleaseModification12.2(25)SGSupport for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines If trunk-status logging event is not configured at the interface level, the global trunk-status setting takes effect for each interface.

Examples This example shows how to globally enable link status messaging on each interface: Switch# config terminal

> Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# logging event trunk-status global Switch(config)# end Switch#

Related Commands	Command	Description	
	logging event trunk-status global (global configuration)	Enables the trunk-status event messaging on an interface.	

logging event trunk-status (interface configuration)

To enable the trunk-status event messaging on an interface, use the **logging event trunk-status** command. Use the **no** form of this command to disable the trunk-status event messaging. Use the **logging event trunk-status use-global** command to apply the global trunk-status setting.

logging event trunk-status

no logging event trunk-status

logging event trunk-status use-global

- **Defaults** Global trunk-status messaging is enabled.
- **Command Modes** Interface configuration mode

 Command History
 Release
 Modification

 12.2(25)SG
 Support for this command was introduced on the Catalyst 4500 series switch.

Usage GuidelinesTo enable system logging of interface state-change events on a specific interface, enter the
logging event trunk-status command in interface configuration mode.

To enable system logging of interface state-change events on all interfaces in the system, enter the **logging event trunk-status use-global** command in global configuration mode. All interfaces without the state change event configuration use the global setting.

Examples This example shows how to enable logging event state-change events on interface gi11/1:

Switch# config terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# interface gill/1 Switch(config-if)# logging event trunk-status Switch(config-if)# end Switch#

This example shows how to turn off logging event trunk status regardless of the global setting:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gill/1
Switch(config-if)# no logging event trunk-status
Switch(config-if)# end
Switch#
```

This example shows how to enable the global event trunk-status setting on interface gi11/1:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gill/1
Switch(config-if)# logging event trunk-status use-global
Switch(config-if)# end
Switch#
```

Related Commands

Command	Description
logging event trunk-status global (global configuration)	Enables the trunk-status event messaging on an interface.

mac access-list extended

To define the extended MAC access lists, use the **mac access-list extended** command. To remove the MAC access lists, use the **no** form of this command.

mac access-list extended name

no mac access-list extended name

Syntax Description	name A	ACL to which the entry belongs.			
Defaults	MAC access lists	s are not defined.			
Command Modes	Global configuration mode				
Command History	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				
	{{ <i>src-mac mask</i>	the mac access-list extended <i>name</i> command, you use the [no] {permit deny } any } [<i>dest-mac mask</i>]} [protocol-family {appletalk arp-non-ipv4 decnet ipx rarp-non-ipv4 vines xns }] subset to create or delete entries in a MAC layer access			
	Table 2-7 descrit	bes the syntax of the mac access-list extended subcommands.			
	Table 2-7	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.			
	src-mac mask	Source MAC address in the form: source-mac-address source-mac-address-mask.			
	any	Specifies any protocol type.			

Subcommand	Description
dest-mac mask	(Optional) Destination MAC address in the form: dest-mac-address dest-mac-address-mask.
protocol-family	(Optional) Name of the protocol family. Table 2-8 lists which packets are mapped to a particular protocol family.

Table 2-7 mac access-list extended Subcommands (continued)

Table 2-8 describes 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 0x6000-0x6009, 0x8038-0x8042 Decnet 0x8137-0x8138 Ipx 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

Table 2-8 Mapping an Ethernet Packet to a Protocol Family

When you enter the *src-mac mask* or *dest-mac mask* value, follow these guidelines:

- Enter the MAC addresses as three 4-byte values in dotted hexadecimal format such as 0030.9629.9f84.
- Enter the 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.
- The access list entries are scanned in the order that 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
Switch(config-ext-macl)# end
Switch#
```

L

Related Commands	Command	Description
	show vlan access-map	Displays VLAN access map information.

mac-address-table aging-time

To configure the aging time for the 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]

Related Commands	Command	Description			
	0	Description			
	Switch(config))			
	Switch(config)# mac-address-table aging-time 0				
	This example shows how to disable aging:				
	Switch(config)# mac-address-table aging-time 400 Switch(config)#				
xamples	This example shows how to configure the aging time to 400 seconds:				
lsage Guidelines	If you do not enter a VLAN, the change is applied to all routed-port VLANs. Enter 0 seconds to disable aging.				
	12.1(12c)EW	Support for extended addressing was added.			
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.			
Command History	Release	Modification			
	Global configu				
Command Modes	Global configu	ration mode			
Defaults	Aging time is so	et to 300 seconds.			
		to 4094.			
	vlan vlan_id	(Optional) Single VLAN number or a range of VLANs; valid values are from 1			
Syntax Description	seconds	Aging time in seconds; valid values are 0 and from 10 to 1000000 seconds.			

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 th	ne "ip" protocol bu	cket.	
	other		Specifies the	ne "other" protocol	bucket.	
Defaults	The group lear	ning feature	e is disable	1.		
Command Modes	Global configu	ration mod	e			
Command History	Release	Modifie	cation			
	12.2(18)EW	Suppor	t for this co	ommand was introc	uced on the Catalyst 4500 series switch	•
Usage Guidelines	The entries wit	-	' and "othe	r" protocol buckets	are created according to the protocol of	f the
	that might belo Therefore, any unicasted to that	ng to either traffic dest at MAC add e incoming	the "ip" of ined to this ress, rather traffic fron	r the "other" protoc MAC address and than flooded. This	rotocols command, an incoming MAC a col bucket, is learned on both protocol b belonging to any of the protocol bucket reduces the unicast Layer 2 flooding tha a different protocol bucket than the traft	uckets. ts is t might
Examples	This example s protocol bucke		he MAC ad	dresses are initiall	y assigned to either the "ip" or the "othe	er"
		es ddress	type	protocols	port	
	1 0001. 1 0003. 1 0003. 1 0003. 1 0003. 1 0003. 1 0003.	0000.5000 0234.6616 3178.ec0a 4700.24c3 4716.f475 4748.75c5 47f0.d6a3 47f6.a91a	dynamic dynamic	other ip assigned ip ip ip ip	GigabitEthernet1/1 GigabitEthernet3/1 GigabitEthernet3/1 GigabitEthernet3/1 GigabitEthernet3/1 GigabitEthernet3/1 GigabitEthernet3/1	

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	_	GigabitEthernet3/1
1	0007.e997.7e8f	dynamic	ip	GigabitEthernet3/1
1	0007.e9ad.5e24	dynamic	ip	GigabitEthernet3/1
1	000b.5f0a.f1d8	dynamic	-	GigabitEthernet3/1
1	000b.fdf3.c498	dynamic	-	GigabitEthernet3/1
1	0010.7be8.3794	-	assigned	GigabitEthernet3/1
1	0012.436f.c07f	dynamic	-	GigabitEthernet3/1
1	0050.0407.5fel	dynamic	-	GigabitEthernet3/1
1	0050.6901.65af	dynamic		GigabitEthernet3/1
1	0050.da6c.81cb	dynamic		GigabitEthernet3/1
1	0050.dad0.af07	dynamic	-	GigabitEthernet3/1
1	00a0.ccd7.20ac	dynamic	-	GigabitEthernet3/1
1	00b0.64fd.1c23	dynamic		GigabitEthernet3/1
1	00b0.64fd.2d8f	-	assigned	GigabitEthernet3/1
1	00d0.b775.c8bc	dynamic	-	GigabitEthernet3/1
1	00d0.b79e.de1d	dynamic	-	GigabitEthernet3/1
1	00e0.4c79.1939	dynamic	-	GigabitEthernet3/1
1	00e0.4c7b.d765	dynamic	-	GigabitEthernet3/1
1	00e0.4c82.66b7	dynamic	-	GigabitEthernet3/1
1	00e0.4c8b.f83e	dynamic	-	GigabitEthernet3/1
1	00e0.4cbc.a04f	dynamic	-	GigabitEthernet3/1
1	0800.20cf.8977	dynamic	-	GigabitEthernet3/1
1	0800.20f2.82e5	dynamic	ip	GigabitEthernet3/1
Switch#				

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
_____+
                                               GigabitEthernet1/1
  1 0000.0000.5000 dynamic ip,other
  1 0001.0234.6616 dynamic ip,other
                                                GigabitEthernet3/1
  1 0003.4700.24c3 dynamic ip,other
                                                GigabitEthernet3/1
      0003.4716.f475 dynamic ip,other
                                                GigabitEthernet3/1
  1
      0003.4748.75c5 dynamic ip,other
                                                GigabitEthernet3/1
  1
  1
       0003.47c4.06c1 dynamic ip,other
                                                 GigabitEthernet3/1
  1
       0003.47f0.d6a3
                     dynamic ip,other
                                                 GigabitEthernet3/1
                    dynamic ip,other
  1
       0003.47f6.a91a
                                                 GigabitEthernet3/1
       0003.ba0e.24a1 dynamic ip,other
  1
                                                 GigabitEthernet3/1
       0003.fd63.3eb4 dynamic ip,other
                                                 GigabitEthernet3/1
  1
  1
       0004.2326.18a1 dynamic ip,other
                                                 GigabitEthernet3/1
       0004.5a5d.de53 dynamic ip,other
                                                 GigabitEthernet3/1
  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
       0004.5a5f.08f6
                     dynamic ip,other
                                                 GigabitEthernet3/1
  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
witch#				

Switch#

mac-address-table notification

To enable MAC address notification on a switch, use the **mac-address-table notification** command. To return to the default setting, use the **no** form of this command

mac-address-table notification {**change** [**history-size** *hs_value*] | [**interval** *intv_value*]] | [**mac-move**] | [**threshold** [**limit** *percentage*] | [**interval** *time*]}

no mac-address-table notification {**change** [**history-size** *hs_value*] | [**interval** *intv_value*]] | [**mac-move**] | [**threshold** [**limit** *percentage*] | [**interval** *time*]}

Syntax Description	change	(Optional) Specifies enabling MAC change notification.		
	history-size hs_value	(Optional) Maximum number of entries in the MAC change notification history table. The range is 0 to 500 entries.		
	interval intv_value	(Optional) Notification trap interval, set interval time between two consecutive traps. The range is 0 to 2,147,483,647 seconds.		
	mac-move	(Optional) Specifies enabling MAC move notification.		
	threshold	(Optional) Specifies enabling MAC threshold notification.		
	limit percentage(Optional) Specifies the percentage of MAT utilization threshold; values are from 1 to 100 percent.			
	interval time	(Optional) Specifies the time between MAC threshold notifications; valid values are greater than or equal to 120 seconds.		
Defaults	MAC address notification feature is disabled. The default MAC change trap interval value is 1 second. The default number of entries in the history table is 1. MAC move notification is disabled. MAC threshold monitoring feature is disabled. The default limit is 50 percent. The default time is 120 seconds.			
Command Modes	Global configuration me	ode		
Command History	Release Mod	ification		
	12.2(31)SG Supp	port for this command was introduced on the Catalyst 4500 series switch.		

Usage Guidelines	We can enable the MAC change notification feature by using the mac address-table notification change command. We must also enable MAC notification traps on an interface by using the snmp trap mac-notification change interface configuration command and configure the switch to send MAC change traps to the NMS by using the snmp-server enable traps mac-notification global configuration command.		
	When the <i>history-size</i> option is configure table is created.	ed, the existing MAC change history table is deleted, and a new	
Examples	This example shows how to set the MAC	C address notification history table size to 300 entries:	
	<pre>Switch(config)# mac-address-table notification change history-size 300 Switch(config)#</pre>		
	This example shows how to set the MAC address notification interval time to 1250 seconds:		
	Switch(config)# mac-address-table n Switch(config)#	otification change interval 1250	
Related Commands	Command	Description	
	clear mac-address-table	Clears the global counter entries from the Layer 2 MAC address table.	
	mac-address-table notification	Enables MAC address notification on a switch.	
	snmp-server enable traps	Enables SNMP notifications.	
	snmp trap mac-notification change	Enables SNMP MAC address notifications.	

mac-address-table static

To configure the 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 the 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	mac-addr	MAC address; optional when using the no form of this command.
	vlan vlan-id	VLAN and valid VLAN number; valid values are from 1 to 4094.
	interface type	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 h	as no default settings.
Command Modes	Global configura	tion mode
Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switches.
Usage Guidelines	The output interf If you do not ente	AC address is installed, it is associated with a port. Face specified must be a Layer 2 interface and not an SVI. For a protocol type, an entry is automatically created for each of the four protocol types. Form of this command does not remove the system MAC addresses.
	When removing a removed automat	a MAC address, entering interface <i>int</i> is optional. For unicast entries, the entry is tically. For multicast entries, if you do not specify an interface, the entire entry is n specify the selected ports to be removed by specifying the interface.
Examples	-	ows how to add the static entries to the MAC address table:
Related Commands	Switch(config)#	Description
neialeu commanus	eemana	

macro apply cisco-desktop

To enable the 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 ha	s no default settings.	
Command Modes	Interface configur	ration mode	
Command History	Release	Modification	
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.	
Usage Guidelines	This command ca	n only be viewed and applied; it cannot be modified.	
		isting configuration on the interface does not conflict with the intended macro fore you apply the macro, clear the configuration on the interface with the default nd.	
Examples	This example sho	ws how to enable the Cisco-recommended features and settings on port fa2/1:	
	Switch(config)# interface FastEthernet2/1 Switch(config-if)# macro apply cisco-desktop \$AVID 50 Switch(config-if)#		
	The contents of th	is macro are as follows:	
	<pre># 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</pre>		

Related Commands	Command	Description
	macro apply cisco-phone	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop and a Cisco IP phone.
	macro apply cisco-router	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a router.
	macro apply cisco-switch	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to another switch.

macro apply cisco-phone

To enable the 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 access_vlanic	d Specifies an access VLAN ID.		
	\$VVID voice_vlanid	Specifies a voice VLAN ID.		
Defaults	This command has no default settings.			
Command Modes	Interface configuratio	n mode		
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 on	ly be viewed and applied; it cannot be modified.		
		ng configuration on the interface does not conflict with the intended macro you apply the macro, clear the configuration on the interface with the default		
Examples	This example shows h	now 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)#			
	The contents of this m	nacro are as follows:		
	<pre># and voice VLAN (V # Recommended value switchport access v switchport mode acc</pre>	for access vlan (AVID) should not be 1\ lan \$AVID [access_vlan_id] ess		
	<pre># different from da # Recommended value</pre>	VLAN (VVID) value which should be ta VLAN for voice vlan (VVID) should not be 1 an \$VVID [voice_vlan_id]		
	<pre># Enable port secur # addressees One switchport port-sec</pre>	ity limiting port to a 3 MAC for desktop and two for phone		
	SWITCHDORT DORT-SAC			

switchport port-security aging type inactivity
Enable auto-gos to extend trust to attached Cisco phone
auto gos voip cisco-phone
Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable@

Related Commands

Command	Description
macro apply cisco-desktop	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop.
macro apply cisco-router	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a router.
macro apply cisco-switch	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to another switch.

macro apply cisco-router

To enable the 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	\$NVID <i>native_vl</i>	anid Specifies a native VLAN ID.
Defaults	This command ha	s no default settings.
Command Modes	Interface configur	ration mode
Command History	Release	Modification
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Usage Guidelines		n only be viewed and applied; it cannot be modified.
	configuration. Be	isting configuration on the interface does not conflict with the intended macro fore you apply the macro apply cisco-router command, clear the configuration on the default interface command.
Examples	Switch(config)#	ws how to enable the Cisco-recommended features and settings on port fa2/1: interface FastEthernet2/1 E) # macro apply cisco-router \$NVID 80 E) #
	The contents of th	is macro are as follows:
	<pre>switchport trunk # Define unique # Recommended va switchport trunk # Update the al: # includes data, # switchport trunk # Hardcode trunk # Hardcode trunk # Hardcode speed switchport mode switchport noneg speed 100 duplex full</pre>	d and duplex to router trunk gotiate to trust this interface

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	Command	Description
	macro apply cisco-desktop	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop.
	macro apply cisco-phone	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop and a Cisco IP phone.
	macro apply cisco-router	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a router.
	macro apply cisco-switch	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to another switch.

macro apply cisco-switch

To enable the 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 native_vlani	<i>d</i> Specifies a native VLAN ID.	
Defaults	This command has no	o default settings.	
Command Modes	Interface configuration	on mode	
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 or	nly be viewed and applied; it cannot be modified.	
-		ng configuration on the interface does not conflict with the intended macro e you apply this macro, clear the configuration on the interface with the default	
Examples	This example shows l	how to enable the Cisco-recommended features and settings on port fa2/1:	
	<pre>Switch(config)# interface FastEthernet2/1 Switch(config-if)# macro apply cisco-switch \$NVID 45 Switch(config-if)#</pre>		
	The contents of this r	nacro are as follows:	
	<pre># Recommended value switchport trunk na # Update the allowe # includes data, vo # switchport trunk # Hardcode trunk ar # speed up converge switchport mode tru switchport nonegoti # Configure qos to auto qos voip trust # 802.1w defines th</pre>	ncapsulation dotlq tive VLAN on trunk ports e for native vlan (NVID) should not be 1 ative vlan \$NVID [native_vlan_id] ed VLAN range (VRANGE) such that it bice and native VLANs allowed vlan \$VRANGE and disable negotiation to ence unk iate trust this interface	

Related Commands	Command	Description
	macro apply cisco-desktop	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop.
	macro apply cisco-phone	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop and a Cisco IP phone.
	macro apply cisco-router	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a router.

macro global apply cisco-global

To apply the system-defined default template to the switch, use the **macro global apply cisco-global** global configuration command on the switch stack or on a standalone switch.

macro global apply cisco-global

Syntax Description This command has no keywords or variables.

Defaults This command has no default setting.

Command Modes Global configuration mode

Command History	Release	Modification
	12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switch.

Examples These examples show how to apply the system-defined default to the switch:

Switch(config)#macro global apply cisco-global Changing VTP domain name from gsg-vtp to [smartports] Device mode already VTP TRANSPARENT. Switch(config)#

macro global apply system-cpp

To apply the control plane policing default template to the switch, use the **macro global apply system-cpp** global configuration command on the switch stack or on a standalone switch.

macro global apply system-cpp

Syntax Description This command has no keywords or variables.

Command Modes Global configuration mode

Command History	Release	Modification
	12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switch.
Usage Guidelines	This command is n	ot supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.

Examples These examples show how to apply the system-defined default to the switch:

Switch (config)# **macro global apply system-cpp** Switch (config)#

Related Commands	Command	Description	
	macro global apply cisco-global	Applies the system-defined default template to the switch.	
	macro global description	Enters a description about the macros that are applied to the switch.	

macro global description

To enter a description about the macros that are applied to the switch, use the **macro global description** global configuration command on the switch stack or on a standalone switch. Use the no form of this command to remove the description.

macro global description text

no macro global description text

Syntax Description	description <i>text</i> Enter a description about the macros that are applied to the switch.			
Defaults	This command has	no default setting.		
Command Modes	Global configuratio	on mode		
Command History	Release	Modification		
	12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switch.		
Usage Guidelines	Use the description keyword to associate comment text, or the macro name, with a switch. When multiple macros are applied on a switch, the description text will be from the last applied macro.			
	This example shows how to add a description to a switch:			
	Switch(config)# macro global description udld aggressive mode enabled			
	You can verify your settings by entering the show parser macro description privileged EXEC command.			
Related Commands	Command	Description		
neialeu cummanns				

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

 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. The 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#
```

Γ

Related Commands	Command	Description	
	auto-sync	Enables automatic synchronization of the configuration files in NVRAM.	

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 acl-number	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 acl-name	Selects an IP ACL by name.			
	mac address acl-name	Selects one or more MAC ACLs for a VLAN access-map sequence.			
Defaults	This command has no d	efault settings.			
Command Modes	VLAN access-map				
Command History	Release Mod	ification			
	12.1(12c)EW Supp	bort 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 <i>Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide</i> 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:				
		access-map ganymede 10 map)# match ip address 13 map)#			

Related Commands	Command	Description
	show vlan access-map	Displays the contents of a VLAN access map.
	vlan access-map	Enters VLAN access-map command mode to create a VLAN access map.

match (class-map configuration)

To define the match criteria for a class map, use the **match** class-map configuration command. To remove the match criteria, use the **no** form of this command.

Non-Supervisor Engine 6-E

- **match** {**access-group** *acl-index-or-name* | **cos** *cos-list* | [**lp**] **dscp** *dscp-list* | [**lp**] **precedence** *ip-precedence-list*
- **no match** {**access-group** *acl-index-or-name* | **cos** *cos-list* | [**lp**] **dscp** *dscp-list* | [**lp**] **precedence** *ip-precedence-list*

Supervisor Engine 6-E and Catalyst 4900M chassis

match {access-group *acl-index-or-name* | cos *cos-list* | [**lp**] dscp *dscp-list* | [**lp**] precedence *ip-precedence-list* | qos-group *value* | protocol [**ip** | **ipv6** | arp]

no match {access-group *acl-index-or-name* | **cos** *cos-list* | [**lp**] **dscp** *dscp-list* | [**lp**] **precedence** *ip-precedence-list* | **qos-group** *value* | **protocol** [**ip** | **ipv6** | **arp**]

Syntax Description	access-group acl-index-or-name	Number or name of an IP standard or extended access control list (ACL) or MAC ACL. For an IP standard ACL, the ACL index range is 1 to 99 and 1300 to 1999. For an IP extended ACL, the ACL index range is 100 to 199 and	
	cos cos-list	2000 to 2699.List of up to four Layer 2 class of service (CoS) values to match against a packet. Separate each value with a space. The range is 0 to 7.	
	[lp] dscp dscp-list	(Optional) IP keyword. It specifies that the match is for IPv4 packets only. If not used, the match is for both IPv4 and IPv6 packets.	
		List of up to eight IP Differentiated Services Code Point (DSCP) values to match against a packet. Separate each value with a space. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value.	
	[lp] precedence <i>ip-precedence-list</i>	(Optional) IP keyword. It specifies that the match is for IPv4 packets only. If not used, the match is for both IPv4 and IPv6 packets.	
		List of up to eight IP-precedence values to match against a packet. Separate each value with a space. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.	
	qos-group value	Specifies the internally generated qos-group value assigned to a packet on the input qos classification.	
	protocol ip	Specifies IP in the Ethernet header. The match criteria are supported on the Supervisor Engine 6-E and Catalyst 4900M chassis. Though visible in the command-line help strings the only protocol types supported are IP, IPv6, and ARP.	

	protocol ipv6	Specifies IPv6 in the Ethernet header. The match criteria are supported on the Supervisor Engine 6-E and Catalyst 4900M chassis. Though visible in the command-line help strings the only protocol types supported are IP, IPv6, and ARP.
	protocol arp	Specifies ARP in the Ethernet header. The match criteria are supported on the Supervisor Engine 6-E and Catalyst 4900M chassis. Though visible in the command-line help strings the only protocol types supported are IP, IPv6, and ARP.
Defaults	No match criteria ar	re defined.
Command Modes	Class-map configura	ation
Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switches.
	12 2(10) 5 5	
	12.2(40)SG	Added support for the Supervisor Engine 6-E and Catalyst 4900M chassis.
Usage Guidelines	12.2(46)SG	Added support for the Supervisor Engine 6-E and Catalyst 4900M chassis. Added support for the match protocol arp command on the Supervisor Engine 6-E and Catalyst 4900M chassis. match command, you must first enter the class-map global configuration comman
Usage Guidelines	12.2(46)SG Before entering the to specify the name to specify which fie specified criteria, th quality of service (Q For the match ip ds a mnemonic name for	Added support for the match protocol arp command on the Supervisor Engine 6-E and Catalyst 4900M chassis. match command, you must first enter the class-map global configuration comman of the class whose match criteria you want to establish. The match command is use lds in the packets are examined to classify the packets. If a packet matches the e packet is considered a member of the class and is forwarded according to the QoS) specifications set in the traffic policy. cp <i>dscp-list</i> or the match ip precedence <i>ip-precedence-list</i> command, you can enter or a commonly used value. For example, you can enter the match ip dscp af11
Jsage Guidelines	12.2(46)SG Before entering the to specify the name to specify which fie specified criteria, th quality of service (Q) For the match ip ds a mnemonic name for command, which is precedence critical	Added support for the match protocol arp command on the Supervisor Engine 6-E and Catalyst 4900M chassis. match command, you must first enter the class-map global configuration comman of the class whose match criteria you want to establish. The match command is use lds in the packets are examined to classify the packets. If a packet matches the e packet is considered a member of the class and is forwarded according to the QoS) specifications set in the traffic policy. cp <i>dscp-list</i> or the match ip precedence <i>ip-precedence-list</i> command, you can enter the same as entering the match ip dscp 10 command. You can enter the match ij command, which is the same as entering the match ip precedence ? command to commonics, enter the match ip dscp ? or the match ip precedence ? command to
Jsage Guidelines	12.2(46)SGBefore entering the to specify the name to specify which fie specified criteria, th quality of service (QFor the match ip ds a mnemonic name fic command, which is precedence critical a list of supported n see the command-line To match only IPv6	Added support for the match protocol arp command on the Supervisor Engine 6-E and Catalyst 4900M chassis. match command, you must first enter the class-map global configuration comman of the class whose match criteria you want to establish. The match command is use lds in the packets are examined to classify the packets. If a packet matches the e packet is considered a member of the class and is forwarded according to the QoS) specifications set in the traffic policy. cp <i>dscp-list</i> or the match ip precedence <i>ip-precedence-list</i> command, you can enter the same as entering the match ip dscp 10 command. You can enter the match ip command , which is the same as entering the match ip precedence ? command to commonics, enter the match ip dscp ? or the match ip precedence ? command to
Jsage Guidelines	12.2(46)SG Before entering the to specify the name of to specify which fie specified criteria, th quality of service (Q For the match ip ds a mnemonic name for command, which is precedence critical a list of supported n see the command-lin To match only IPv6 packets you can use	Added support for the match protocol arp command on the Supervisor Engine 6-E and Catalyst 4900M chassis. match command, you must first enter the class-map global configuration comman of the class whose match criteria you want to establish. The match command is use lds in the packets are examined to classify the packets. If a packet matches the e packet is considered a member of the class and is forwarded according to the QoS) specifications set in the traffic policy. cp <i>dscp-list</i> or the match ip precedence <i>ip-precedence-list</i> command, you can enter or a commonly used value. For example, you can enter the match ip dscp af11 the same as entering the match ip dscp 10 command. You can enter the match ij command, which is the same as entering the match ip precedence ? command to nemonics, enter the match ip dscp ? or the match ip precedence ? command to ne help strings. packets, you must use the match protocol ipv6 command. To match only IPv4
Jsage Guidelines	12.2(46)SG Before entering the to specify the name to specify which fie specified criteria, th quality of service (Q For the match ip ds a mnemonic name for command, which is precedence critical a list of supported n see the command-lin To match only IPv6 packets you can use To match only ARP You can configure th	Added support for the match protocol arp command on the Supervisor Engine 6-E and Catalyst 4900M chassis. match command, you must first enter the class-map global configuration comman of the class whose match criteria you want to establish. The match command is use lds in the packets are examined to classify the packets. If a packet matches the e packet is considered a member of the class and is forwarded according to the QoS) specifications set in the traffic policy. cp <i>dscp-list</i> or the match ip precedence <i>ip-precedence-list</i> command, you can enter or a commonly used value. For example, you can enter the match ip dscp af11 the same as entering the match ip dscp 10 command. You can enter the match ip command, which is the same as entering the match ip precedence ? command to nemonics, enter the match ip dscp ? or the match ip precedence ? command to ne help strings. packets, you must use the match protocol ipv6 command. To match only IPv4 either the ip prefix or the protocol ip keyword.
Usage Guidelines	12.2(46)SGBefore entering the to specify the name to specify which fie specified criteria, th quality of service (QFor the match ip ds a mnemonic name fic command, which is precedence critical a list of supported n see the command-line To match only IPv6 packets you can use To match only ARP You can configure th <i>ip-precedence-list</i> c	Added support for the match protocol arp command on the Supervisor Engine 6-E and Catalyst 4900M chassis. match command, you must first enter the class-map global configuration command of the class whose match criteria you want to establish. The match command is use lds in the packets are examined to classify the packets. If a packet matches the e packet is considered a member of the class and is forwarded according to the QoS) specifications set in the traffic policy. cp <i>dscp-list</i> or the match ip precedence <i>ip-precedence-list</i> command, you can enter or a commonly used value. For example, you can enter the match ip dscp af11 the same as entering the match ip dscp 10 command. You can enter the match ij command, which is the same as entering the match ip precedence <i>5</i> command. For anemonics, enter the match ip dscp ? or the match ip precedence ? command to ne help strings. packets, you must use the match protocol ipv6 command. To match only IPv4 either the ip prefix or the protocol ip keyword . packets, you must use the match protocol arp command. he match cos <i>cos-list</i> , match ip dscp <i>dscp-list</i> , match ip precedence

Packets that do not meet any of the matching criteria are classified as members of the default traffic class. You configure it by specifying **class-default** as the class name in the **class** policy-map configuration command. For more information, see the "class" section on page 2-29.

Examples

This example shows how to create a class map called *class2*, which matches all the inbound traffic with DSCP values of 10, 11, and 12:

```
Switch# configure terminal
Switch(config)# class-map class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# exit
Switch#
```

This example shows how to create a class map called *class3*, which matches all the inbound traffic with IP-precedence values of 5, 6, and 7 for both IPv4 and IPv6 traffic:

```
Switch# configure terminal
Switch(config)# class-map class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# exit
Switch#
```

This example shows how to delete the IP-precedence match criteria and to classify traffic using acl1:

```
Switch# configure terminal
Switch(config)# class-map class2
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# no match ip precedence
Switch(config-cmap)# match access-group acl1
Switch(config-cmap)# exit
Switch#
```

This example shows how to specify a class-map that applies only to IPv6 traffic on a Supervisor Engine 6-E:

```
Switch# configure terminal
Switch(config)# class-map match all ipv6 only
Switch(config-cmap)# match dscp af21
Switch(config-cmap)# match protocol ipv6
Switch(config-cmap)# exit
Switch#
```

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

Related Commands	Command	Description
	class-map	Creates a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode.
	show class-map	Displays class map information.

L

match flow ip

To specify match criteria to treat flows with a unique source or destination address as new flows, use the **match flow ip** command. To disable this function, use the **no** form of this command.

match flow ip {source-address [ip destination-address ip protocol L4 source-address L4 destination-address] | destination-address}

no match flow ip {source-address [ip destination-address ip protocol L4 source-address L4 destination-address] | destination-address}

Syntax Description	source-address Establishes a new flow from a flow with a unique IP source address.				
	ip destination-address ip protocol L4 source-address L4 destination-addressComprises the full flow keyword; treats each flow with unique destination, protocol, and Layer 4 source and destination address flow.				
	destination-add	Iress Establishes a new flow from a flow with a unique IP destination address.			
Defaults	None.				
Command Modes	class-map config	guration submode			
Command History	Release Modification				
	12.2(25)EW Support for this command was introduced on the Catalyst 4500 series switch.				
	12.2(25)SGSupport for the full flow option was added.				
Usage Guidelines	When you specif new flow.	fy the source-address keyword, each flow with a unique source address is treated as a			
	When you specify the destination-address keyword, each flow with a unique destination address is treated as a new flow.				
	A policy map is called a <i>flow-based</i> policy map when you configure the flow keywords on the class map that it uses. To attach a flow-based policy map as a child to an aggregate policy map, use the service-policy command.				
Note	The match flow command is available on the Catalyst 4500 series switch only when Supervisor Engine VI (WS-X4516-10GE) is present.				

Examples

This example shows how to create a flow-based class map associated with a source address:

```
Switch(config)# class-map match-all c1
Switch(config-cmap)# match flow ip source-address
Switch(config-cmap)# end
Switch#
Switch# show class-map c1
Class Map match-all c1 (id 2)
Match flow ip source-address
Switch#
```

This example shows how to create a flow-based class map associated with a destination address:

```
Switch(config)# class-map match-all c1
Switch(config-cmap)# match flow ip destination-address
Switch(config-cmap)# end
Switch#
Switch# show class-map c1
Class Map match-all c1 (id 2)
Match flow ip destination-address
Switch#
```

Assume there are two active flows on the Fast Ethernet interface 6/1 with source addresses 192.168.10.20 and 192.168.10.21. The following example shows how to maintain each flow to 1 Mbps with an allowed burst value of 9000 bytes:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map c1
Switch(config-cmap) # match flow ip source-address
Switch(config-cmap)# exit
Switch(config) # policy-map p1
Switch(config-pmap) # class c1
Switch(config-pmap-c)# police 1000000 9000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet6/1
Switch(config-if)# service-policy input p1
Switch(config-if)# end
Switch# write memory
Switch# show policy-map interface
FastEthernet6/1
 Service-policy input: p1
   Class-map: c1 (match-all)
     15432182 packets
     Match: flow ip source-address
     police: Per-interface
       Conform: 64995654 bytes Exceed: 2376965424 bytes
   Class-map: class-default (match-any)
     0 packets
     Match: any
       0 packets
```

This example shows two active flows on the Fast Ethernet interface 6/1 with destination addresses of 192.168.20.20 and 192.168.20.21. The following example shows how to maintain each flow to 1 Mbps with an allowed burst value of 9000 bytes:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map cl
Switch(config-cmap)# match flow ip destination-address
Switch(config-cmap)# exit
Switch(config)# policy-map pl
Switch(config-pmap)# class cl
Switch(config-pmap-c)# police 1000000 9000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet6/1
Switch(config-if)# service-policy input pl
Switch(config-if)# end
Switch(config-if)# end
```

```
Switch# show policy-map interface
FastEthernet6/1
```

Service-policy input: p1

```
Class-map: c1 (match-all)

2965072 packets

Match: flow ip destination-address

police: Per-interface

Conform: 6105636 bytes Exceed: 476652528 bytes

Class-map: class-default (match-any)

0 packets

Match: any

0 packets
```

Switch#

Assume there are two active flows as shown below on the Fast Ethernet interface 6/1:

SrcIp	DstIp	IpProt	SrcL4Port	DstL4Port
192.168.10.10	192.168.20.20	20	6789	81
192.168.10.10	192.168.20.20	20	6789	21

With the following configuration, each flow is policed to a 1000000 bps with an allowed 9000-byte burst value.



If you use the **match flow ip source-address/destination-address** command, these two flows are consolidated into one flow because they have the same source and destination address.

```
Switch# conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map cl
Switch(config-cmap)# match flow ip source-address ip destination-address ip protocol l4
source-port l4 destination-port
Switch(config-cmap)# exit
Switch(config)# policy-map pl
Switch(config-pmap)# class cl
Switch(config-pmap-c)# police 1000000 9000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastEthernet 6/1
```

```
Switch(config-if)# service-policy input p1
Switch(config-if)# end
Switch# write memory
Switch# show policy-map interface
FastEthernet6/1
class-map c1
   match flow ip source-address ip destination-address ip protocol 14 source-port 14
destination-port
1
policy-map p1
   class c1
      police 1000000 bps 9000 byte conform-action transmit exceed-action drop
!
interface FastEthernet 6/1
 service-policy input p1
Switch# show class-map c1
 Class Map match-all c1 (id 2)
   Match flow ip source-address ip destination-address ip protocol 14 source-port 14
destination-port
Switch# show policy-map p1
  Policy Map p1
   Class c1
      police 1000000 bps 9000 byte conform-action transmit exceed-action drop
Switch# show policy-map interface
 FastEthernet6/1
  Service-policy input: p1
    Class-map: c1 (match-all)
      15432182 packets
      Match: flow ip source-address ip destination-address ip protocol 14 source-port 14
destination-port
      police: Per-interface
        Conform: 64995654 bytes Exceed: 2376965424 bytes
    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets
Switch#
```

Related Commands

Command	Description
service-policy (interface configuration)	Attaches a policy map to an interface.
show class-map	Displays class map information.
show policy-map	Displays information about the policy map.
show policy-map interface	Displays the statistics and configurations of the input and output policies that are attached to an interface.

mdix auto

To enable the automatic medium-dependent interface crossover (auto-MDIX) feature on the interface, use the **mdix auto** command. When auto-MDIX is enabled, the interface automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately. Use the no form of this command to disable auto-MDIX.

mdix auto

no mdix auto

Syntax Description This command has no arguments or keywords.

Defaults Auto-MDIX is enabled.

Command Modes interface configuration

Command History	Release	Modification
	12.2(31)SGA	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(46)SG	Added supported and unsupported linecard information to the usage guidelines.

Usage Guidelines Linecards that support auto-MDIX configuration on their copper media ports include: WS-X4124-RJ45, WS-X4148-RJ with hardware revision 3.0 or later, WS-X4232-GB-RJ with hardware revision 3.0 or later, WS-X4920-GE-RJ45 and WS-4648-RJ45V+E.

Linecards that support auto-MDIX by default when port auto-negotiation enabled and cannot be turned off using an **mdix** CLI command include: WS-X4448-GB-RJ45, WS-X4548-GB-RJ45, WS-X4424-GB-RJ45, and WS-X4412-2GB-T.

Linecards that cannot support auto-MDIX functionality, either by default or CLI commands, include: WS-X4548-GB-RJ45V, WS-X4524-GB-RJ45V, WS-X4506-GB-T, WS-X4148-RJ, WS-X4248-RJ21V, WS-X4248-RJ45V, WS-X4224-RJ45V, and WS-X4232-GB-RJ.

When you enable auto-MDIX on an interface, you must also set the interface speed to be autoneogiated so that the feature operates correctly.

When auto-MDIX (and autonegotiation of speed) is enabled on one or both of connected interfaces, link up occurs even if the cable type (straight-through or crossover) is incorrect.

Examples This example shows how to enable auto MDIX on a port: Switch# configure terminal

```
Switch(config)# interface FastEthernet6/3
Switch(config-if)# speed auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```
Related Commands	Command	Description
	speed	Configures the interface speed.
	show interfaces	Displays traffic on a specific interface.
	show interfaces capabilities	Displays the interface capabilities for an interface or for all the interfaces on a switch.
	show interfaces status	Displays the interface status.

media-type

To select the connector for a dual-mode capable port, use the media-type command.

media-type {rj45 | sfp} Syntax Description rj45 Uses the RJ-45 connector. Uses the SFP connector. sfp Defaults sfp **Command Modes** Interface configuration mode **Command History** Release Modification 12.2(20)EWA Support for this command was introduced for the WS-X4306-GB-T module and the WS-X4948 chassis. **Usage Guidelines** This command is supported on all ports on the WS-X4306-GB-T module and ports 1/45-48 on the WS-X4948 chassis. Entering the show interface capabilities command provides the Multiple Media Types field, which displays the value **no** if a port is not dual-mode capable and lists the media types (sfp and rj45) for dual-mode capable ports. **Examples** This example shows how to configure port 5/45 on a WS-X4948 chassis to use the RJ-45 connector: Switch(config)# interface gigabitethernet 5/45 Switch(config-if) # media-type rj45

mode

To set the redundancy mode, use the **mode** command.

mode {rpr | sso}

Syntax Description	rpr	Specifies RPR mode.
	SSO	Specifies SSO mode.
Defaults		500 series switches that are configured with Supervisor Engine II+, Supervisor Engine IV, or Engine V, the defaults are as follows:
	• SSO, if th	ne supervisor engine is using Cisco IOS Release 12.2(20)EWA.
	• RPR, if the well as 12	the supervisor engine is using Cisco IOS Release $12.1(12c)$ EW through $12.2(18)$ EW, as $2.1(xx)$ E.
	earlier both s	are upgrading the current supervisor engine from Cisco IOS Release 12.2(18)EW or an r release to 12.2(20)EWA, and the RPR mode has been saved to the startup configuration, supervisor engines will continue to operate in RPR mode after the software upgrade. To use mode, you must manually change the redundancy mode to SSO.
Command Modes	Redundancy c	onfiguration
Command History	Release	Modification
	12.2(20)EWA	Support for this command was introduced on the Catalyst 4500 series switch.
Usage Guidelines	RPR and SSO	mode are not supported on Catalyst 4500 series switches that are configured with
	Supervisor En	
	Supervisor En	
	Supervisor En The mode cor	ngine 2.
	Supervisor En The mode con Follow these g • You must	ngine 2. mmand can be entered only from within redundancy configuration mode. guidelines when configuring your system to RPR or SSO mode: use identical Cisco IOS images and supervisor engines to support RPR and SSO mode. ncy may not work due to differences between the Cisco IOS release and supervisor engine
	Supervisor En The mode con Follow these g • You must Redundar capabilitie	ngine 2. mmand can be entered only from within redundancy configuration mode. guidelines when configuring your system to RPR or SSO mode: use identical Cisco IOS images and supervisor engines to support RPR and SSO mode. ncy may not work due to differences between the Cisco IOS release and supervisor engine
	Supervisor En The mode con Follow these g • You must Redundar capabilitie • Any mode • If you per	ngine 2. mmand can be entered only from within redundancy configuration mode. guidelines when configuring your system to RPR or SSO mode: use identical Cisco IOS images and supervisor engines to support RPR and SSO mode. ncy may not work due to differences between the Cisco IOS release and supervisor engine es.
	Supervisor En The mode con Follow these g • You must Redundar capabilitie • Any mode • If you per resets dur	ngine 2. mmand can be entered only from within redundancy configuration mode. guidelines when configuring your system to RPR or SSO mode: use identical Cisco IOS images and supervisor engines to support RPR and SSO mode. ncy may not work due to differences between the Cisco IOS release and supervisor engine es. ules that are not online at the time of a switchover are reset and reloaded on a switchover rform an OIR of the module within 60 seconds before a stateful switchover, the module ring the stateful switchover and the port states are restarted. tables are cleared on a switchover. Routed traffic is interrupted until route tables
	 Supervisor En The mode con Follow these g You must Redundar capabilitie Any mode If you per resets dur The FIB t reconverged 	ngine 2. mmand can be entered only from within redundancy configuration mode. guidelines when configuring your system to RPR or SSO mode: use identical Cisco IOS images and supervisor engines to support RPR and SSO mode. ncy may not work due to differences between the Cisco IOS release and supervisor engine es. ules that are not online at the time of a switchover are reset and reloaded on a switchover rform an OIR of the module within 60 seconds before a stateful switchover, the module ring the stateful switchover and the port states are restarted. tables are cleared on a switchover. Routed traffic is interrupted until route tables

Examples

This example shows how to set the redundancy mode to SSO:

Switch(config)# redundancy
Switch(config-red)# mode sso
Switch(config-red)#

Related Commands	Command	Description
	redundancy	Enters the redundancy configuration mode.
	redundancy force-switchover	Forces a switchover from the active to the standby supervisor engine.
	show redundancy	Displays redundancy facility information.
	show running-config	Displays the running configuration of a switch.

monitor session

To enable the 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 |

 $\begin{array}{l} \textbf{GigabitEthernet} interface-number} \ [encapsulation \{isl \mid dot1q\}] \ [ingress [vlan vlan_id] \\ [learning]] \} \mid \{remote vlan vlan_id\} \mid \{source \{interface \{FastEthernet interface-number \mid GigabitEthernet interface-number \mid Port-channel interface-number\} \} \mid [vlan vlan_id] \\ \hline [GigabitEthernet interface-number \mid Port-channel interface-number] \} \mid [vlan vlan_id] \\ \hline [remote vlan vlan_id] \mid \{cpu [queue queue_id \mid acl \{input \{error \{rx\} \mid log \{rx\} \mid punt \{rx\} \mid rx\} \} \mid output \{error \{rx\} \mid forward \{rx\} \mid log \{rx\} \mid punt \{rx\} \mid rx\} \mid adj-same-if \{rx\} \mid all \\ \hline [rx] \mid bridged \{1 \{rx\} \mid 2 \{rx\} \mid 3 \{rx\} \mid 4 \{rx\} \mid rx\} \mid control-packet \{rx\} \mid mu-exceeded \\ \hline [rx] \mid routed \{forward \{1 \{rx\} \mid 2 \{rx\} \mid 3 \{rx\} \mid 4 \{rx\} \mid rx\} \mid received \{1 \{rx\} \mid 2 \{rx\} \mid 3 \\ \hline [rx] \mid 4 \{rx\} \mid rx\} \mid rx] \mid rpf-failure \{rx\} \mid unknown-sa \{rx\}] \}] [, |-|rx| tx \mid both] \} | \{filter \\ \hline [ip access-group [name \mid id]] \{vlan vlan_id [, |-]\} \mid \{packet-type \{good \mid bad\}\} | \\ \ \{address-type \{unicast \mid multicast \mid broadcast\} [rx \mid tx \mid both] \} \end{array}$

no monitor 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 | acl {input {error {rx} | log {rx} | punt {rx} | rx}} | output {error {rx} | forward {rx} | log {rx} | punt {rx} | adj-same-if {rx} | all {rx} | bridged {1 {rx} | 2 {rx} | 3 {rx} | 4 {rx} | rx} | control-packet {rx} | mu-exceeded {rx} | routed {forward {1 {rx} | 2 {rx} | 3 {rx} | 4 {rx} | rx} | received {1 {rx} | 2 {rx} | 3 {rx} | 4{rx} | rx} | rx | both]} | {filter {ip access-group [name | id]}{vlan vlan_id [, -]} | {packet-type {good | bad}} | {address-type {unicast | multicast | broadcast} [rx | tx | both]}

Supervisor Engine 6-E and Catalyst 4900M chassis

- 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 | acl { input {copy {rx} | error {rx} | forward
 {rx} | punt {rx} | rx} }] output {copy {rx} | error {rx} | forward {rx} | punt {rx} | rx} | all
 {rx} | control-packet {rx} | esmp {rx} | l2-forward { adj-same-if {rx} | bridge-cpu {rx} |
 ip-option {rx} | ipv6-scope-check-fail {rx} | l2-src-index-check-fail {rx} | rx} |
 l3-forward { forward {rx} | glean {rx} | receive {rx} | rx} mtu-exceeded {rx} |
 unknown-port-vlan-mapping {rx} | unknown-sa {rx}]} [, | | rx | tx | both]} | {filter {ip
 access-group [name | id]}{vlan vlan_id [, | -]} | {packet-type {good | bad}} | {address-type
 {unicast | multicast | broadcast} [rx | tx | both]}
- no monitor session {destination interface {FastEthernet interface-number |
 GigabitEthernet interface-number } [encapsulation {isl | dot1q }] [ingress [vlan vlan_id]
 [learning]] } | {remote vlan vlan_id} | {source {cpu{both | queue | rx | tx} | interface
 {FastEthernet interface-number | GigabitEthernet interface-number | Port-channel
 interface-number} } | [vlan vlan_id] | {remote vlan vlan_id} | {cpu [queue queue_id | acl
 {input {copy {rx} | error {rx} | forward {rx} | punt {rx} | rx} } }] output {copy {rx} | error
 {rx} | forward {rx} | punt {rx} | rx} | all {rx} | control-packet {rx} | esmp {rx} | 12-forward

 $\{ adj-same-if \{rx\} | bridge-cpu \{rx\} | ip-option \{rx\} | ipv6-scope-check-fail \{rx\} | 12-src-index-check-fail \{rx\} | mcast-rpf-fail \{rx\} | non-arpa \{rx\} | router-cpu \{rx\} | ttl-expired \{rx\} | ucast-rpf-fail \{rx\} | rx\} | 13-forward {forward {rx} | glean {rx} | rceeive {rx} | rx} mtu-exceeded {rx} | unknown-port-vlan-mapping {rx} | unknown-sa {rx}] } [, | -| rx | tx | both] \} | {filter {ip access-group [name | id]}{vlan vlan_id [, |-]} | {packet-type {good | bad} } | {address-type {unicast | multicast | broadcast} [rx | tx | both] }$

Syntax Description	session	Number of a SPAN session; valid values are from 1 to 6.
	destination	Specifies a SPAN destination.
	interface	Specifies an interface.
	FastEthernet interface-number	Specifies a Fast Ethernet module and port number; valid values are from 1 to 6.
	GigabitEthernet interface-number	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 vlan_id	(Optional) Specifies the VLAN; valid values are from 1 to 4094.
	learning	(Optional) Enables host learning on ingress-enabled destination ports.
	remote vlan vlan_id	Specifies an RSPAN source or destination session on a switch.
	source	Specifies a SPAN source.
	Port-channel interface-number	Specifies a port-channel interface; valid values are from 1 to 64.
	сри	Causes traffic received or sent from the CPU to be copied to the destination of the session.
	queue <i>queue_id</i>	(Optional) 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 64, or by the following names: all, control-packet, esmp, mtu-exceeded, unknown-port-vlan-mapping, unknown-sa, acl input, acl input copy, acl input error, acl input forward, acl input punt, acl output, acl output copy, acl output error, acl output forward, acl output punt, 12-forward, adj-same-if, bridge-cpu, ip-option, ipv6-scope-check-fail, 12-src-index-check-fail, mcast-rpf-fail, non-arpa, router-cpu, ttl-expired, ucast-rpf-fail, 13-forward, forward, glean, receive.
	acl	(Optional) Specifies input and output ACLs; valid values are from 14 to 20.
	input	Specifies input ACLs; valid values are from 14 to 16.
	error	Specifies the ACL software errors.
	log/copy	Specifies packets for ACL logging.
	punt	Specifies packets punted due to overflows.
	rx	Specifies monitoring received traffic only.

output	Specifies output ACLs; valid values are from 17 to 20.
l2-forward	(Optional) Layer 2 or Layer 3 exception packets.
bridge-cpu	Specifies packets bridged to CPU.
ip-option	Specifies packets with an IP option.
ipv6-scope-check-fail	Specifies IPv6 packets with scope-check failures.
l2-src-index-check-fail	Specifies IP packets with mismatched SRC MAC and SRC IP addresses.
mcast-rpf-fail	Specifies IPv4/IPv6 multicast RPF failures.
non-arpa	Specifies packets with non-ARPA encapsulation.
router-cpu	Specifies software routed packets.
ttl-expired	Specifies IPv4 routed pacekts exceed TTL.
adj-same-if	Specifies packets routed to the incoming interface.
bridged	Specifies Layer 2 bridged packets.
1	Specifies packets with the highest priority.
2	Specifies packets with the a high priority.
3	Specifies packets with the a medium priority.
4	Specifies packets with the a low priority.
ucast-rpf-fail	Specifies IPv4/IPv6 Unicast RPF failures.
all	(Optional) all queues.
13-forward	(Optional) Layer 3 packets.
forward	Specifies special Layer 3 forwards tunnel encapsulation.
glean	Specifies special Layer 3 forwards glean.
receive	Specifies packets addressed to a port.
control-packet	(Optional) Layer 2 control packets.
esmp	(Optional) ESMP packets.
mtu-exceeded	(Optional) Output Layer 3 interface MTU exceeded.
routed	Specifies Layer 3 routed packets.
received	Specifies packets addressed to a port.
rpf-failure	Specifies Multicast RPF failed packets.
unknown-port-vlan-mapping	(Optional) Packets with missing port-VLAN mapping.
unknown-sa	(Optional) Packets with missing source-IP-addresses.
,	(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.
ip access-group	(Optional) Specifies an IP access group filter, either a name or a number.
name	(Optional) Specifies an IP access list name.

	id		(Optional) Specifies an IP access list number. Valid values are 1 to 199 for an IP access list and 1300 to 2699 for an IP expanded access list.	
	vlan vlan_id		(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 u broadcast	nicast multicast	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 trans	Packets are transmitted untagged out the destination port; ingress and learning are disabled.		
Command Modes	Global configura	ation mode		
Command History	Release	Modification		
Command History	Release 12.1(8a)EW		ommand was introduced on the Catalyst 4500 series switch.	
Command History		Support for this co	ng directions within a single-user session and extended VLAN	
Command History	12.1(8a)EW	Support for this co Support for differ addressing was ad Support for ingres	ng directions within a single-user session and extended VLAN	
Command History	12.1(8a)EW 12.1(11b)EW	Support for this co Support for differ addressing was ad Support for ingres filtering, and CPU	ng directions within a single-user session and extended VLAN ded. s packets, encapsulation specification, packet and address type	
Command History	12.1(8a)EW 12.1(11b)EW 12.1(19)EW	Support for this co Support for differ addressing was ad Support for ingres filtering, and CPU Support for remot was added.	ng directions within a single-user session and extended VLAN ded. s packets, encapsulation specification, packet and address type source sniffing enhancements was added.	
Command History	12.1(8a)EW 12.1(11b)EW 12.1(19)EW 12.1(20)EW	Support for this co Support for differ addressing was ad Support for ingress filtering, and CPU Support for remot was added. Support for an IP	ng directions within a single-user session and extended VLAN ded. s packets, encapsulation specification, packet and address type source sniffing enhancements was added. e SPAN and host learning on ingress-enabled destination ports	

interface to a session that already has a destination interface that is configured, you will get an error. You must first remove a SPAN destination interface before changing the SPAN destination to a different interface.

Beginning in Cisco IOS Release 12.1(12c)EW, you can configure sources from different directions within a single user session.

<u>Note</u>

Beginning in Cisco IOS 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 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.

The packet-type filters are supported only in the Rx direction. You can specify both Rx- and Tx-type filters and multiple-type filters at the same time (for example, you can use **good** and **unicast** to only sniff nonerror unicast frames). As with VLAN filters, if you do not specify the type, the session will sniff all packet types.

The **queue** identifier allows sniffing for only traffic that is sent or received on the specified CPU queues. The queues may be identified either by number or by name. The queue names may contain multiple numbered queues for convenience.

Examples

This example shows how to configure IP access group 100 on a SPAN session:

```
Switch# configure terminal
Switch(config)# monitor session 1 filter ip access-group 100
Switch(config)# end
Switch(config)#
```

This example shows how to add a source interface to a SPAN session:

```
Switch# configure terminal
Switch(config)# monitor session 1 source interface fa2/3
Switch(config)# end
Switch(config)#
Switch(config)#
Switch(config)#
```

This example shows how to configure the sources with different directions within a SPAN session:

```
Switch# configure terminal
Switch(config)# monitor session 1 source interface fa2/3 rx
Switch(config)# monitor session 1 source interface fa2/2 tx
Switch(config)# end
```

This example shows how to remove a source interface from a SPAN session:

```
Switch# configure terminal
Switch(config)# no monitor session 1 source interface fa2/3
Switch(config)# end
```

This example shows how to limit SPAN traffic to VLANs 100 through 304:

```
Switch# configure terminal
Switch(config)# monitor session 1 filter vlan 100 - 304
Switch(config)# end
```

This example shows how to configure RSPAN VLAN 20 as the destination:

```
Switch# configure terminal
Switch(config)# monitor session 2 destination remote vlan 20
Switch(config)# end
```

This example shows how to use queue names and queue number ranges for the CPU as a SPAN source on Supervisor Engine 6-E:

```
Switch# configure terminal
Switch(config)# monitor session 2 source cpu queue control-packet rx
Switch(config)# monitor session 3 source cpu queue 10 rx
Switch(config)# end
```



For Supervisor Engine 6-E and Catalyst 4900M chassis, control-packet is mapped to queue 10.

Related Commands	Command	Description
	show monitor	Displays information about the SPAN session.

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	bytes	Byte size; valid values are from 1500 to 9198.	
Defaults	The default sett	ings are as follows:	
	• Jumbo fram	es are disabled	
	• 1500 bytes	for all ports	
Command Modes	Interface config	uration mode	
Command History	Release	Modification	
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switches.	
	 EtherChannels. Jumbo frames are not available for stub-based ports. The baby giants feature uses the global system mtu <i>size</i> command to set the global baby giant MTU. It allows all stub-based port interfaces to support an 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, t	but the per-interface mtu command takes precedence.	
Examples	This example shows how to specify an MTU of 1800 bytes:		
	Switch(config) Switch(config-	<pre># interface GigabitEthernet 1/1 if)# mtu 1800</pre>	
Related Commands	Command	Description	
	system mtu	Sets the maximum Layer 2 or Layer 3 payload size.	

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	-	pecifies the name of the MST region. The name can be any string with a maximum ngth of 32 characters.
Defaults	The MST region na	me 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.
Examples		red to be in different MST regions if the region names are different.
Examples	This example show Switch(config-mst Switch(config-mst	
Related Commands	Command	Description
	instance	Maps a VLAN or a set of VLANs to an MST instance.
	revision	Sets the MST configuration revision number.
	show spanning-tro	ee mst Displays MST protocol information.
	spanning-tree mst configuration	Enters the MST configuration submode.

pagp learn-method

To learn the input interface of the 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.
efaults	Aggregation port is	enabled.
ommand Modes	Interface configura	tion mode
command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Examples	I.	s how to enable physical port address learning within the bundle: # pagp learn-method physical-port #
	1	s how to enable aggregation port address learning within the bundle: # pagp learn-method aggregation-port #
Related Commands	Command	Description
		Displays information about the port channel.

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	priority	Port priority number; valid values are from 1 to 255.
Defaults	Port priority is	set to 128.
Command Modes	Interface config	uration mode
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 J	priority, the better the chances are that the port will be selected in the hot standby mode.
Examples	This example sl	nows how to set the port priority:
	Switch(config- Switch(config-	<pre>if)# pagp port-priority 45 if)#</pre>
Related Commands	Command	Description
	pagp learn-me	thod Learns the input interface of the incoming packets.
	show pagp	Displays information about the port channel.

passive-interface

To disable sending routing updates on an interface, use the **passive-interface** command. To reenable the sending of routing updates, use the **no** form of this command.

passive-interface [[**default**] {*interface-type interface-number*}] | {**range** *interface-type interface-type interface-type interface-number*}

no passive-interface [[**default**] {*interface-type interface-number*}] | {**range** *interface-type interface-type interface-number*}]

Syntax Description	default	(Optional) All interfaces become passive.	
	interface-type	Specifies the interface type.	
	interface-number	Specifies the interface number.	
	range range	Specifies the range of subinterfaces being configured; see the "Usage Guidelines" section.	
Defaults	Routing updates are	sent on the interface.	
Command Modes	Router configuration		
Command History	Release	Modification	
	12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switch.	
Usage Guidelines	You can use the passive-interface range command on the following interfaces: FastEthernet, GigabitEthernet, VLAN, Loopback, Port-channel, 10-GigabitEthernet, and Tunnel. When you use the passive-interface range command on a VLAN interface, the interface should be the existing VLAN SVIs. To display the VLAN SVIs, enter the show running config command. The VLANs that are not displayed cannot be used in the passive-interface range command.		
		ntered with the passive-interface range command are applied to all the existing	
	Before you can use a	macro, you must define a range using the define interface-range command.	
	-	inges that are made to a port range through the passive-interface range command nning-configuration as individual passive-interface commands.	
	You can enter the range in two ways:		
	• Specifying up to	five interface ranges	
	• Specifying a pre-	viously defined macro	
	• Specifying a previously defined macro You can either specify the interfaces or the name of an interface-range macro. An interface consist of the same interface type, and the interfaces within a range cannot span across the		

You can define up to five interface ranges on a single command; separate each range with a comma:

interface range gigabitethernet 5/1-20, gigabitethernet4/5-20.

Use this format when entering the *port-range*:

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

You cannot specify both a macro and an interface range in the same command. After creating a macro, you can enter additional ranges. 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 **range** range value. This makes the command similar to the **passive-interface** *interface-number* command.

Note

The range keyword is only supported in OSPF, EIGRP, RIP, and ISIS router mode.

If you disable the sending of routing updates on an interface, the particular subnet will continue to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

The **default** keyword sets all interfaces as passive by default. You can then configure individual interfaces where adjacencies are desired using the **no passive-interface** command. The **default** keyword is useful in Internet service provider (ISP) and large enterprise networks where many of the distribution routers have more than 200 interfaces.

For the Open Shortest Path First (OSPF) protocol, OSPF routing information is neither sent nor received through the specified router interface. The specified interface address appears as a stub network in the OSPF domain.

For the Intermediate System-to-Intermediate System (IS-IS) protocol, this command instructs IS-IS to advertise the IP addresses for the specified interface without actually running IS-IS on that interface. The **no** form of this command for IS-IS disables advertising IP addresses for the specified address.

Note

For IS-IS you must keep at least one active interface and configure the interface with the **ip router isis** command.

Enhanced Interior Gateway Routing Protocol (EIGRP) is disabled on an interface that is configured as passive although it advertises the route.

Examples

The following example sends EIGRP updates to all interfaces on network 10.108.0.0 except GigabitEthernet interface 1/1:

```
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# router eigrp 109
Switch(config-router)# network 10.108.0.0
Switch(config-router)# passive-interface gigabitethernet 1/1
Switch(config-router)#
```

The following configuration enables IS-IS on Ethernet interface 1 and serial interface 0 and advertises the IP addresses of Ethernet interface 0 in its link-state protocol data units (PDUs):

```
Switch(config-if)# router isis Finance
Switch(config-router)# passive-interface Ethernet 0
Switch(config-router)# interface Ethernet 1
Switch(config-router)# ip router isis Finance
Switch(config-router)# interface serial 0
Switch(config-router)# ip router isis Finance
Switch(config-router)# ip router isis Finance
```

The following example sets all interfaces as passive, then activates Ethernet interface 0:

```
Switch(config-if)# router ospf 100
Switch(config-router)# passive-interface default
Switch(config-router)# no passive-interface ethernet0
Switch(config-router)# network 10.108.0.1 0.0.0.255 area 0
Switch(config-router)#
```

The following configuration sets the Ethernet ports 3 through 4 on module 0 and GigabitEthernet ports 4 through 7 on module 1 as passive:

```
Switch(config-if)# router ospf 100
Switch(config-router)# passive-interface range ethernet0/3-4,gigabitethernet1/4-7
Switch(config-router)#
```

permit

To permit an ARP packet based on matches against the DHCP bindings, use the **permit** command. To remove a specified ACE from an access list, use the **no** form of this command

- 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]

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 sender-ip	Specifies that only a specific sender IP address will be accepted.
sender-ip sender-ip-mask	Specifies that a specific range of sender IP addresses will be accepted.
mac	Specifies the sender MAC address.
host sender-mac	Specifies that only a specific sender MAC address will be accepted.
sender-mac sender-mac-mask	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 target-ip	(Optional) Specifies that only a specific target IP address will be accepted.
target-ip target-ip-mask	(Optional) Specifies that a specific range of target IP addresses will be accepted.
mac	Specifies the MAC address values for the ARP responses.
host target-mac	(Optional) Specifies that only a specific target MAC address will be accepted.
target-mac target-mac-mask	(Optional) Specifies that a specific range of target MAC addresses will be accepted.
ranger mare mash	
	ip any host sender-ip sender-ip sender-ip-mask mac host sender-mac sender-mac sender-mac-mask response ip host target-ip target-ip target-ip-mask mac host target-mac target-mac

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	Permit clauses can be added to forward or drop ARP packets based on some matching criteria.		
Examples	-	This example shows a host with a MAC address of 0000.0000.abcd and an IP address of 1.1.1.1. This example shows how to permit both requests and responses from this host:		
	<pre>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</pre>			
	ARP access list s permit ip hos Switch#	static-hosts st 1.1.1.1 mac host 0000.0000.abcd		
Related Commands	Command	Description		
	arp access-list	Defines an ARP access list or adds clauses at the end of a predefined list.		
	deny	Denies an ARP packet based on matches against the DHCP bindings.		
	ip arp inspection	filter vlan Permits ARPs from hosts that are configured for static IP when DAI is enabled and to define an ARP access list and applies it to a VLAN.		

police

To configure the Traffic Policing feature, use the **police** QoS policy-map class configuration command. To remove the Traffic Policing feature from the configuration, use the **no** form of this command.

police {*bps* | *kbps* | *mbps* | *gbps*} [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]

no police {*bps* | *kbps* | *mbps* | *gbps*} [*burst-normal*] [*burst-max*] **conform-action** *action exceed-action action* [*violate-action action*]

Syntax Description	bps	Average rate, in bits per second. Valid values are 32,000 to 32,000,000
	kbps	Average rate, in kilobytes per second. Valid values are 32 to 32,000,000.
	mbps	Average rate, in megabits per second. Valid values are 1 to 32,000.
	gbps	Average rate, in gigabits per second. Valid values are 1 to 32.
	burst-normal	(Optional) Normal burst size, in bytes. Valid values are 64 to 2,596,929,536 Burst value of up to four times the configured rate can be supported.
	burst-max	(Optional) Excess burst size, in bytes. Valid values are 64 to 2,596,929,536 Burst value of upto four times the configured rate can be supported.
	conform-action	Action to take on packets that conform to the rate limit.
	exceed-action	Action to take on packets that exceed the rate limit.
	violate-action	(Optional) Action to take on packets that violate the normal and maximum burst sizes.
	action	Action to take on packets. Specify one of the following keywords:
		• drop —Drops the packet.
		• set-cos-transmit new-ios—Set the class of services (CoS) value to a new value and send the packet. The range is 0 to 7.
		• set-dscp-transmit <i>value</i> —Sets the IP differentiated services code poin (DSCP) value and transmits the packet with the new IP DSCP value setting.
		• set-prec-transmit <i>value</i> —Sets the IP precedence and transmits the packet with the new IP precedence value setting.
		• transmit —Transmits the packet. The packet is not altered.

Defaults This command is disabled by default.

Command ModesPolicy-map class configuration (when specifying a single action to be applied to a market packet)Policy-map class police configuration (when specifying multiple actions to be applied to a marked packet)

Command History	Release	Modification			
	12.2(40)SGThis command was introduced on the Catalyst 4500 series sw				
		using a Supervisor Engine 6E.			
sage Guidelines	Use the police command conformance to the serv	t to mark a packet with different quality of service (QoS) values based on ice-level agreement.			
	Traffic policing will not	be executed for traffic that passes through an interface.			
	Specifying Multiple Action	15			
		ows you to specify multiple policing actions. When specifying multiple policin g the police command, note the following points:			
	• You can specify a maximum of four actions at one time.				
	• You cannot specify <i>drop</i> .	contradictory actions such as conform-action <i>transmit</i> and conform-action			
	Using the Police Command with the Traffic Policing Feature				
	a token bucket algorithm a two-token bucket algo	n be used with Traffic Policing feature. The Traffic Policing feature works with Two types of token bucket algorithms are a single-token bucket algorithm an rithm. A single-token bucket system is used when the violate-action option is token bucket system is used when the violate-action option is specified.			
	Token Bucket Algorithm with One Token Bucket				
	-	gorithm is used when the violate-action option is not specified in the police			
	The conform bucket is in normal burst size).	nitially set to the full size (the full size is the number of bytes specified as the			
	When a packet of a given actions occur:	n size (for example, "B" bytes) arrives at specific time (time "T") the followin			
	current time is T, th	in the conform bucket. If the previous arrival of the packet was at T1 and the e bucket is updated with (T - T1) worth of bits based on the token arrival rate te is calculated as follows:			
	(time between packe	ets <which -="" equal="" is="" t="" t1="" to=""> * policer rate)/8 bytes</which>			
	and the conform act	tes in the conform bucket B is greater than or equal to 0, the packet conforms ion is taken on the packet. If the packet conforms, B bytes are removed from the the conform action is completed for the packet.			
	• If the number of byt	es in the conform bucket B (minus the packet size to be limited) is fewer than (taken.			

Token Bucket Algorithm with Two Token Buckets (Refer to RFC 2697)

The two-token bucket algorithm is used when the violate-action is specified in the police command CLI.

The conform bucket is initially full (the full size is the number of bytes specified as the normal burst size).

The exceed bucket is initially full (the full exceed bucket size is the number of bytes specified in the maximum burst size).

The tokens for both the conform and exceed token buckets are updated based on the token arrival rate, or committed information rate (CIR).

When a packet of given size (for example, "B" bytes) arrives at specific time (time "T") the following actions occur:

• Tokens are updated in the conform bucket. If the previous arrival of the packet was at T1 and the current arrival of the packet is at t, the bucket is updated with T -T1 worth of bits based on the token arrival rate. The refill tokens are placed in the conform bucket. If the tokens overflow the conform bucket, the overflow tokens are placed in the exceed bucket.

The token arrival rate is calculated as follows:

(time between packets <which is equal to T-T1> * policer rate)/8 bytes

- If the number of bytes in the conform bucket B is greater than or equal to 0, the packet conforms and the conform action is taken on the packet. If the packet conforms, B bytes are removed from the conform bucket and the conform action is taken. The exceed bucket is unaffected in this scenario.
- If the number of bytes in the conform bucket B is less than 0, the excess token bucket is checked for bytes by the packet. If the number of bytes in the exceed bucket B is greater than or equal to 0, the exceed action is taken and B bytes are removed from the exceed token bucket. No bytes are removed from the conform bucket.
- If the number bytes in the exceed bucket B is fewer than 0, the packet violates the rate and the violate action is taken. The action is complete for the packet.

Examples Token Bucket Algorithm with One Token Bucket

This example shows how to define a traffic class (using the **class-map** command) and associate the match criteria from the traffic class with the Traffic Policing configuration, which is configured in the service policy (using the **policy-map** command). The **service-policy** command is then used to attach this service policy to the interface.

In this particular example, Traffic Policing is configured with the average rate at 8000 bits per second and the normal burst size at 1000 bytes for all packets leaving Gigabit Ethernet interface 6/1:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map access-match
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# policy-map police-setting
Switch(config-pmap)# class access-match
Switch(config-pmap-c)# police 8000 1000 conform-action transmit exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 6/1
Switch(config-if)# service-policy output police-setting
Switch(config-if)# end
```

In this example, the initial token buckets starts full at 1000 bytes. If a 450-byte packet arrives, the packet conforms because enough bytes are available in the conform token bucket. The conform action (send) is taken by the packet and 450 bytes are removed from the conform token bucket (leaving 550 bytes).

If the next packet arrives 0.25 seconds later, 250 bytes are added to the token bucket ((0.25 * 8000)/8), leaving 800 bytes in the token bucket. If the next packet is 900 bytes, the packet exceeds and the exceed action (drop) is taken. No bytes are taken from the token bucket.

Token Bucket Algorithm with Two Token Buckets Example (Refer to RFC 2697)

In this particular example, Traffic Policing is configured with the average rate at 8000 bits per second, the normal burst size at 1000 bytes, and the excess burst size at 1000 bytes for all packets leaving Gigabit Ethernet interface 6/1.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map access-match
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# policy-map police-setting
Switch(config-pmap)# class access-match
Switch(config-pmap-c)# police 8000 1000 conform-action transmit exceed-action set-qos-transmit 1
violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 6/1
Switch(config-if)# service-policy output police-setting
Switch(config-if)# end
```

In this example, the initial token buckets starts full at 1000 bytes. If a 450-byte packet arrives, the packet conforms because enough bytes are available in the conform token bucket. The conform action (send) is taken by the packet and 450 bytes are removed from the conform token bucket (leaving 550 bytes).

If the next packet arrives 0.25 seconds later, 250 bytes are added to the conform token bucket ((0.25 * 8000)/8), leaving 800 bytes in the conform token bucket. If the next packet is 900 bytes, the packet does not conform because only 800 bytes are available in the conform token bucket.

The exceed token bucket, which starts full at 1000 bytes (as specified by the excess burst size) is then checked for available bytes. Because enough bytes are available in the exceed token bucket, the exceed action (set the QoS transmit value of 1) is taken and 900 bytes are taken from the exceed bucket (leaving 100 bytes in the exceed token bucket.

If the next packet arrives 0.40 seconds later, 400 bytes are added to the token buckets ((.40 * 8000)/8). Therefore, the conform token bucket now has 1000 bytes (the maximum number of tokens available in the conform bucket) and 200 bytes overflow the conform token bucket (because it only 200 bytes were needed to fill the conform token bucket to capacity). These overflow bytes are placed in the exceed token bucket, giving the exceed token bucket 300 bytes.

If the arriving packet is 1000 bytes, the packet conforms because enough bytes are available in the conform token bucket. The conform action (transmit) is taken by the packet and 1000 bytes are removed from the conform token bucket (leaving 0 bytes).

If the next packet arrives 0.20 seconds later, 200 bytes are added to the token bucket ((.20 * 8000)/8). Therefore, the conform bucket now has 200 bytes. If the arriving packet is 400 bytes, the packet does not conform because only 200 bytes are available in the conform bucket. Similarly, the packet does not exceed because only 300 bytes are available in the exceed bucket. Therefore, the packet violates and the violate action (drop) is taken.

Related Commands	Command	Description
	police (percent)	Configures traffic policing on the basis of a percentage of bandwidth available on an interface.
	police (two rates)	Configures traffic policing using two rates, the committed information rate (CIR) and the peak information rate (PIR).
	policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
	service-policy (policy-map class)	Creates a service policy that is a quality of service (QoS) policy within a policy map.
	show policy-map	Displays information about the policy map.
	show policy-map interface	Displays the statistics and configurations of the input and output policies that are attached to an interface.

police (percent)

police (percent)

To configure traffic policing on the basis of a percentage of bandwidth available on an interface, use the **police** command in QoS policy-map class configuration mode. To remove traffic policing from the configuration, use the **no** form of this command.

police cir percent *percent* [**bc** *conform-burst-in-msec*] [**pir percent** *percentage*] [**be** *peak-burst-inmsec*]

no police cir percent *percent* [**bc** *conform-burst-in-msec*] [**pir percent** *percentage*] [**be** *peak-burst-inmsec*]

Syntax Description	cir	Committed information rate. Indicates that the CIR will be used for policing traffic.
	percent	Specifies that a percentage of bandwidth will be used for calculating the CIR.
	percent	Specifies the bandwidth percentage. Valid range is a number from 1 to 100.
	bc	(Optional) Conform burst (bc) size used by the first token bucket for policing traffic.
	conform-burst-in-msec	(Optional) Specifies the bc value in milliseconds. Valid range is a number from 1 to 2000.
	pir	(Optional) Peak information rate (PIR). Indicates that the PIR will be used for policing traffic.
	percent	(Optional) Specifies that a percentage of bandwidth will be used for calculating the PIR.
	percent	(Optional) Specifies the bandwidth percentage. Valid range is a number from 1 to 100.
	be	(Optional) Peak burst (be) size used by the second token bucket for policing traffic.
	peak-burst-in-msec	(Optional) Specifies the be size in milliseconds. Valid range is a number from 1 to 2000.
	action	Action to take on packets. Specify one of the following keywords:
		• drop —Drops the packet.
		• set-cos-transmit new-ios—Set the class of services (CoS) value to a new value and send the packet. The range is 0 to 7.
		• set-dscp-transmit <i>value</i> —Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value setting.
		• set-prec-transmit <i>value</i> —Sets the IP precedence and transmits the packet with the new IP precedence value setting.
		• transmit —Transmits the packet. The packet is not altered.

Command Default This command is disabled by default.

Command Modes	Policy-map class configuration		
Command History	Release	Modification	
	12.2(40)SG	This command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6E.	
Usage Guidelines	This command calculates the cir and pir on the basis of a percentage of the maximum amount of bandwidth available on the interface. When a policy map is attached to the interface, the equivalent cir and pir values in bits per second (bps) are calculated on the basis of the interface bandwidth and the percent value entered with this command. The show policy-map interface command can then be used to verify the bps rate calculated.		
	The calculated cir and pir bps rates must be in the range of 32,000 and 32,000,000,000 bps. If the are outside this range, the associated policy map cannot be attached to the interface. If the interface bandwidth changes (for example, more is added), the bps values of the cir and the pir are recalcul on the basis of the revised amount of bandwidth. If the cir and pir percentages are changed after the policy map is attached to the interface, the bps values of the cir and pir are recalculated.		
		o allows you to specify the values for the conform burst size and the peak burst size you want bandwidth to be calculated as a percentage, the conform burst size and the st be specified in milliseconds (ms).	
Examples	This example shows how to configure traffic policing using a CIR and a PIR based on a percentage of bandwidth on Gigabit interface 6/2. In this example, a CIR of 20 percent and a PIR of 40 percent have been specified. Additionally, an optional bc value and be value (300 ms and 400 ms, respectively) have been specified.		
	Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# policy-map policy1 Switch(config-pmap)# class-map class1 Switch(config-pmap-c)# police cir percent 20 bc 3 ms pir percent 40 be 4 ms Switch(config-pmap-c)# exit Switch(config-pmap-c)# exit Switch(config-pmap-c)# interface gigabitethernet 6/2 Switch(config-if)# service-policy output policy Switch(config-if)# end		

police rate

police rate

L

To configure single or dual rate policer, use the **police rate** command in policy-map configuration mode. To remove traffic policing from the configuration, use the **no** form of this command.

Syntax for Bytes Per Second

- **police rate** units **bps** [**burst** burst-in-bytes **bytes**] [**peak-rate** peak-rate-in-bps **bps**] [**pack-burst** peak-burst-in-bytes **bytes**]
- **no police rate** *units* **bps** [**burst** *burst-in-bytes* **bytes**] [**peak-rate** *peak-rate-in-bps* **bps**] [**pack-burst** *peak-burst-in-bytes* **bytes**]

Syntax for Percent

police rate percent percentage [burst ms ms] [peak-rate percent percentage] [pack-burst ms ms]

no police rate percent percentage [burst ms ms] [peak-rate percent percentage] [pack-burst ms ms]

Syntax Description	units	Specifies the traffic police rate in bits per second. Valid range is 32,000 to 32,000,000.
	bps	(Optional) Bits per second (bps) will be used to determine the rate at which traffic is policed.
		Note If a rate is not specified, traffic is policed via bps.
	burst <i>burst-in-bytes</i> bytes	(Optional) Specifies the burst rate, in bytes, will be used for policing traffic. Valid range is from 64 to 2,596,929,536.
	peak-rate peak-rate-in-bps bps	(Optional) Specifies the peak burst value, in bytes, for the peak rate. Valid range is from 32,000 to 32,000,000,000.
	peak-burst peak-burst-in-bytes bytes	(Optional) Specifies the peak burst value, in bytes, will be used for policing traffic. If the police rate is specified in bps, the valid range of values is 64 to 2,596,929,536.
	percent	(Optional) A percentage of interface bandwidth will be used to determine the rate at which traffic is policed.
	percentage	(Optional) Bandwidth percentage. Valid range is a number from 1 to 100.
	burst ms ms	(Optional) Burst rate, in milliseconds, will be used for policing traffic. Valid range is a number from 1 to 2,000.
	peak-rate percent percentage	(Optional) A percentage of interface bandwidth will be used to determine the PIR. Valid range is a number from 1 to 100.
	peak-burst ms ms	(Optional) Peak burst rate, in milliseconds, will be used for policing traffic. Valid range is a number from 1 to 2,000.

Command Default This command is disabled by default.

Command Modes	Policy-map configuration		
Command History	Release	Modification	
	12.2(40)SG	This command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6E.	
Usage Guidelines	Use the police rate command to limit traffic on the basis of pps, bps, or a percentage of interface bandwidth.		
	If the police rat on the basis of	te command is issued, but the a rate is not specified, traffic that is destined will be policed bps.	
Examples	This example shows how to configure policing on a class to limit traffic to an average rate of 1,500,000 bps:		
	Switch(config Switch(config Switch(config Switch(config)# class-map c1 -cmap)# match access-group 140 -cmap)# exit)# policy-map p1 -pmap)# class c1 -pmap-c)# police rate 1500000 burst 500000	
Related Commands	Switch(config	-pmap-c)# exit	
kelated Commands	policy-map	Description Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.	
	show policy-m	Displays information about the policy map.	

police (two rates)

L

To configure traffic policing using two rates, the committed information rate (CIR) and the peak information rate (PIR), use the **police** command in policy-map configuration mode. To remove two-rate traffic policing from the configuration, use the **no** form of this command.

- police cir cir [bc conform-burst] pir pir [be peak-burst] [conform-action action [exceed-action action]]]
- **no police cir** *cir* [**bc** *conform-burst*] **pir** *pir* [**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**exceed-action** *action*]]]

Syntax Description	cir	Committed information rate (CIR) at which the first token bucket is updated.
	cir	Specifies the CIR value in bits per second. The value is a number from 32,000 to 32,000,000,000.
	bc	(Optional) Conform burst (bc) size used by the first token bucket for policing.
	conform-burst	(Optional) Specifies the bc value in bytes. The value is a number from 64 to 2,596,929,536.
	pir	Peak information rate (PIR) at which the second token bucket is updated.
	pir	Specifies the PIR value in bits per second. The value is a number from 32,000 to 32,000,000,000.
	be	(Optional) Peak burst (be) size used by the second token bucket for policing.
	peak-burst	(Optional) Specifies the peak burst (be) size in bytes. The value is a number from 64 to 2,596,929,536.
	conform-action	(Optional) Action to take on packets that conform to the CIR and PIR.
	exceed-action	(Optional) Action to take on packets that conform to the PIR but not the CIR.
	violate-action	(Optional) Action to take on packets exceed the PIR.
	action	(Optional) Action to take on packets. Specify one of the following keywords:
		• drop —Drops the packet.
		• set-cos-transmit new-ios—Set the class of services (CoS) value to a new value and send the packet. The range is 0 to 7.
		• set-dscp-transmit <i>new-dscp</i> —Sets the IP differentiated services code point (DSCP) value and sends the packet with the new IP DSCP value setting.
		• set-prec-transmit <i>new-prec</i> —Sets the IP precedence and sends the packet with the new IP precedence value setting.
		• transmit —Sends the packet with no alteration.

Command Default This command is disabled by default.

Command Modes Policy-map configuration

Command History	Release	Modification
	12.2(40)SG	This command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6E.
Jsage Guidelines	Refer to RFC 2	698-Two Rate Three Color Marker.
		policing uses two token buckets—Tc and Tp—for policing traffic at two independent following points about the two token buckets:
		en bucket is updated at the CIR value each time a packet arrives at the two-rate policer. en bucket can contain up to the confirm burst (Bc) value.
	• The Tp token bucket is updated at the PIR value each time a packet arrives at the two-rate policer. The Tp token bucket can contain up to the peak burst (Be) value.	
	Updating Token I	Buckets
	The following s	scenario illustrates how the token buckets are updated:
	buckets at time	bytes arrives at time t. The last packet arrived at time t1. The CIR and the PIR token t are represented by $Tc(t)$ and $Tp(t)$, respectively. Using these values and in this scenario, ets are updated as follows:
	Tc(t) = min	n(CIR * (t-t1) + Tc(t1), Bc)
	Tp(t) = mir	h(PIR * (t-t1) + Tp(t1), Be)
	Marking Traffic	
	-	blicer marks packets as either conforming, exceeding, or violating a specified rate. The s (using a packet of B bytes) illustrate how a packet is marked:
	• If $B > Tp(t)$), the packet is marked as violating the specified rate.
), the packet is marked as exceeding the specified rate, and the $Tp(t)$ token bucket is $Tp(t) = Tp(t) - B$.
	Otherwise, the p Tp(t)—are upda	packet is marked as conforming to the specified rate, and both token buckets—Tc(t) and ated as follows:
	Tp(t) = Tp(t)	(t) - B
	Tc(t) = Tc(t) - B
	T .	the CIR is 100 kbps, the PIR is 200 kbps, and a data stream with a rate of 250 kbps arrives policer, the packet would be marked as follows:
	• 100 kbps w	yould be marked as conforming to the rate.
	• 100 kbps w	yould be marked as exceeding the rate.
	• 50 kbps wo	ould be marked as violating the rate.
	Marking Packets	s and Assigning Actions Flowchart
	The flowchart i	n Figure 2-1 illustrates how the two-rate policer marks packets and assigns a action (that is, violate, exceed, or conform) to the packet.



Figure 2-1 Marking Packets and Assigning Actions with the Two-Rate Policer

Examples

This example shows how to configure two-rate traffic policing on a class to limit traffic to an average committed rate of 500 kbps and a peak rate of 1 Mbps:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) # class-map police
Switch(config-cmap)# match access-group 101
Switch(config-cmap)# policy-map policy1
Switch(config-pmap) # class police
Switch(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
Switch(config-pmap-c)# interface gigabitethernet 6/1
Switch(config-if)# service-policy output policy1
Switch(config-if) # end
Switch# show policy-map policy1
 Policy Map policy1
  Class police
   police cir 500000 conform-burst 10000 pir 1000000 peak-burst 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
```

Switch#

Traffic marked as conforming to the average committed rate (500 kbps) will be sent as is. Traffic marked as exceeding 500 kbps, but not exceeding 1 Mbps, will be marked with IP Precedence 2 and then sent. All traffic marked as exceeding 1 Mbps will be dropped. The burst parameters are set to 10000 bytes.

Γ

In the following example, 1.25 Mbps of traffic is sent ("offered") to a policer class:

```
Switch# show policy-map interface gigabitethernet 6/1
 GigabitEthernet6/1
  Service-policy output: policy1
   Class-map: police (match all)
   148803 packets, 36605538 bytes
   30 second offered rate 1249000 bps, drop rate 249000 bps
   Match: access-group 101
   police:
    cir 500000 bps, conform-burst 10000, pir 1000000, peak-burst 100000
     conformed 59538 packets, 14646348 bytes; action: transmit
     exceeded 59538 packets, 14646348 bytes; action: set-prec-transmit 2
    violated 29731 packets, 7313826 bytes; action: drop
     conformed 499000 bps, exceed 500000 bps violate 249000 bps
   Class-map: class-default (match-any)
   19 packets, 1990 bytes
    30 seconds offered rate 0 bps, drop rate 0 bps
   Match: any
Switch#
```

The two-rate policer marks 500 kbps of traffic as conforming, 500 kbps of traffic as exceeding, and 250 kbps of traffic as violating the specified rate. Packets marked as conforming to the rate will be sent as is, and packets marked as exceeding the rate will be marked with IP Precedence 2 and then sent. Packets marked as violating the rate are dropped.

policy-map

To create or modify a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode, use the **policy-map** global configuration command. To delete an existing policy map and to return to global configuration mode, use the **no** form of this command.

policy-map policy-map-name

configuration commands.

no policy-map policy-map-name

Syntax Description	policy-map-name	Name of the policy map.
Defaults	No policy maps are de	efined.
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(40)SG	Added support for the Supervisor Engine 6-E and Catalyst 4900M chassis.
Usage Guidelines	policy-map command the policy-map comm	blicies for classes whose match criteria are defined in a class map, use the I to specify the name of the policy map to be created or modified. After you enter hand, the switch enters policy-map configuration mode. You can configure or these for that policy map and decide how to treat the classified traffic.
	These configuration commands are available in policy-map configuration mode:	
	• class : defines the classification match criteria for the specified class map. For more information, see the "class" section on page 2-29.	
	• description : describes the policy map (up to 200 characters).	
	• exit: exits policy-map configuration mode and returns you to global configuration mode.	
	• no : removes a previously defined policy map.	
	To return to global cor the end command.	nfiguration mode, use the exit command. To return to privileged EXEC mode, use
	•	ss policies in a policy map only if the classes have match criteria defined for them. h criteria for a class, use the class-map global configuration and match class-map

Examples

This example shows how to create a policy map called *policy1*. When attached to the ingress direction, it matches all the inbound traffic defined in *class1*, sets the IP DSCP to 10, and polices the traffic at an average rate of 1 Mbps and bursts at 20 KB. Traffic exceeding the profile is marked down to a DSCP value obtained from the policed-DSCP map and then sent. This policer action is applicable on all Catalyst 4500 Supervisors except the Supervisor Engine 6-E and Catalyst 4900M chassis.

```
Switch# configure terminal
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set ip dscp 10
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch#
```

This example shows how to configure multiple classes in a policy map called "policymap2" on a Supervisor Engine 6-E:

```
Switch# configure terminal
Switch(config)# policy-map policymap2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police 100000 20000 exceed-action
Switch(config-pmap-c)# set-dscp-transmit cs3
Switch(config-pmap-c)# set-cos-transmit 3
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# police cir 32000 pir 64000 conform-action transmit exceed-action
Switch(config-pmap-c)# police cir 32000 pir 64000 conform-action transmit exceed-action
Switch(config-pmap-c)# set-dscp-transmit cs3 violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# exit
```

This example shows how to delete the policy map called "policymap2":

```
Switch# configure terminal
Switch(config)# no policy-map policymap2
Switch#
```

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

Related Commands	Command	Description
	class	Specifies the name of the class whose traffic policy you want to create or change.
	class-map	Creates a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode.
	policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
	service-policy (interface configuration)	Attaches a policy map to an interface or applies different QoS policies on VLANs that an interface belongs to.
	show policy-map	Displays information about the policy map.

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 the "Usage Guidelines" section for mor				
		information.			
Defaults	Load distribution on the source XOR destination IP address is enabled.				
Command Modes	Global configuration mode				
Command History	Release	Modification			
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.			
Usage Guidelines	The following	values are valid for the load-distribution method:			
-	• 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 the destination IP address:				
	Switch(config)# port-channel load-balance dst-ip Switch(config)#				
	This example shows how to set the load-distribution method to the source XOR destination IP address:				
	Switch(config)# port-channel load-balance src-dst-port Switch(config)#				

Related Commands	Command	Description
	interface port-channel	Accesses or creates a port-channel interface.
	show etherchannel	Displays EtherChannel information for a channel.
power dc input

To configure the 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	dc input	Specifies the external DC source for both power supply slots.
	watts	Sets the total capacity of the external DC source in watts; valid values are from 300 to 8500.
Defaults	DC power input	t is 2500 W.
Command Modes	Global configur	ration mode
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	•	e is not capable of supporting Power over Ethernet, you will receive this message: mernet not supported on interface Admin
Examples	This example sh	nows how to set the total capacity of the external DC power source to 5000 W:
	Switch(config) Switch(config)	# power dc input 5000 #
Related Commands	Command	Description
	show power	Displays information about the power status.

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-or interfaces.				
	max milliwatt	(Optional) Sets the maximum power that the equipment can consume; valid			
		range is from 2000 to 15400 mW for classic modules. For the			
		WS-X4648-RJ45V-E, the maximum is 20000. For the WS-X4648-RJ45V+E, the maximum is 30000.			
	never	Disables both the detection and power for the inline-power capable interfaces.			
	static	Allocates power statically.			
	consumption milliwa	<i>tt</i> Sets power allocation per interface; valid range is from 4000 to 15400 for classic modules. Any non-default value disables automatic adjustment of power allocation.			
Defaults	The default settings are as follows:				
	• Auto mode for Por	wer over Ethernet is set.			
	• Maximum mW mode is set to 15400. For the WS-X4648-RJ45V-E, the maximum mW is set to 20000. For the WS-X4648-RJ45V+E, the maximum mW is set to 30000.				
	• Default allocation is set to 15400.				
Command Modes	Interface configuration	mode			
Command History	Release Mo	dification			
	12.1(11)EW Sup	port for this command was introduced on the Catalyst 4500 series switch.			
		port added for static power allocation.			
	. , 1	port added for Power over Ethernet.			
	12.2(44)SG Ma	ximum supported wattage increased beyond 15400 for the WS-X4648-RJ45V-E the WS-X4648-RJ45V+E.			
	and	the WS-X4648-RJ45V+E.			

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#
```

This example shows how to pre-allocate Power over Ethernet to 16500 mW for Gigabit Ethernet interface 2/1 regardless of 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 gigabitethernet 2/1
Switch(config-if)# power inline static max 16500
Switch(config-if)# end
Switch#
```

Related Commands	Command	Description
	show power	Displays information about the power status.

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

	milliwatts	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 configur	ation mode		
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.		
	If your interface is not capable of supporting Power over Ethernet, you will receive this message: Power over Ethernet not supported on interface Admin			
	-	nows how to set the Power over Ethernet allocation to use 8000 mW, regardless of any t is received from the powered device:		
	Switch# config Enter configur	Ture terminal Tation commands, one per line. End with CNTL/Z. # power inline consumption default 8000		
Related Commands	Command	Description		
	power inline	Sets the inline-power state for the inline-power-capable interfaces.		
	show power	Displays information about the power status.		

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	redundant	Configures the switch to redundant power management mode.
	combined	Configures the switch to combined power management mode.
Defaults	Redundant pow	ver management mode
Command Modes	Global configu	ration mode
Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch. (Catalyst 4500 series switches only: 4503, 4506, and 4507).

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 use only one power supply.

In redundant mode, the power from a single power supply must provide enough power to support the switch configuration.

Table 2-9 lists the maximum available power for chassis and Power over Ethernet for each power supply.

Table 2-9Available Power

Power Supply	Redundant Mode (W)	Combined Mode (W)
1000 W AC	$System^1 = 1000$	System = 1667
	Inline $= 0$	Inline $= 0$
2800 W AC	System = 1360	System = 2473
	Inline $= 1400$	Inline = 2333

1. The system power includes power for the supervisor engines, all modules, 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	Command	Description
	show power	Displays information about the power status.

port-security mac-address

To configure a secure address on an interface for a specific VLAN or VLAN range, use the **port-security mac-address** command.

port-security mac-address mac_address

Syntax Description	mac_address	mac_addressThe MAC-address that needs to be secured.		
Command Modes	VLAN-range int	erface submode		
Command History	Release	Modification		
	12.2(25)EWA	Support for the	his command was introduced on the Catalyst 4500 series switch.	
Usage Guidelines	•	nd, you can use t	multiple VLANs (for example, a typical trunk port). In conjunction with he port-security mac-address command to specify different addresses	
Examples	This example sh VLANs 2-3:	ows how to conf	figure the secure address 1.1.1 on interface Gigabit Ethernet 1/1 for	
	Switch(config) Switch(config- Switch(config- Switch(config-	ation commands # interface gig if)# switchpor if)# switchpor if)# vlan 2-3 if-vlan-range)	<pre># port-security mac-address 1.1.1</pre>	
Related Commands	Command		Description	
	port-security n sticky	nac-address	Configures a sticky address on an interface for a specific VLAN or VLAN range.	

port-security maximumConfigures the maximum number of addresses on an interface for
a specific VLAN or VLAN range.

port-security mac-address sticky

To configure a sticky address on an interface for a specific VLAN or VLAN range, use the **port-security mac-address sticky** command.

port-security mac-address sticky mac_address

Syntax Description	mac_address	The	MAC-address that needs to be secured.	
Command Modes	VLAN-range interface submode			
Command History	Release	Modification	1	
	12.2(25)EWA	Support for	this command was introduced on the Catalyst 4500 series switch.	
Usage Guidelines	The Sticky feature must be enabled on an interface before you can configure the port-security mac-address sticky command.			
Usage Guidelines	Layer 2 interfaces can be part of multiple VLANs (for example, a typical trunk port). In conjunction with the vlan command, you can use the port-security mac-address sticky command to specify different sticky addresses on different VLANs.			
	The Sticky feature must be enabled on an interface before you can configure the port-security mac-address sticky command.			
	Sticky MAC addresses are addresses that persist across switch reboots and link flaps.			
Examples	This example shows how to configure the sticky address 1.1.1 on interface Gigabit Ethernet 1/1 for VLANs 2-3:			
	Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# interface gigabitethernet1/1 Switch(config-if)# switchport trunk encapsulation dot1q Switch(config-if)# switchport mode trunk Switch(config-if)# vlan 2-3 Switch(config-if-vlan-range)# port-security mac-address sticky 1.1.1 Switch(config-if-vlan-range)# end Switch(config-if-vlan-range)# end			
Related Commands	Command		Description	
	port-security n	nac-address	Configures a secure address on an interface for a specific VLAN or VLAN range.	
	port-security n	navimum	Configures the maximum number of addresses on an interface for	

port-security maximum

To configure the maximum number of addresses on an interface for a specific VLAN or VLAN range, use the **port-security maximum** command.

port-security maximum *max_value*

Syntax Description				
Command Modes				
Command History	Release	Modification		
	12.2(25)EWA	Support for this command was introduced on the Catalyst 4500 series switch.		
Usage Guidelines	the vlan comman	es can be part of multiple VLANs (for example, a typical trunk port). In conjunction with nd, you can use the port-security maximum command to specify the maximum number ses on different VLANs.		
If a specific VLAN on a port is not configured with a maximum value, the maximum config port is used for that VLAN. In this situation, the maximum number of addresses that can be this VLAN is limited to the maximum value configured on the port.				
	Each VLAN can be configured with a maximum count that is greater than the value config port. Also, the sum total of the maximum configured values for all the VLANs can exceed th configured for the port. In either of these situations, the number of MAC addresses secured VLAN is limited to the lesser of the VLAN configuration maximum and the port configura maximum.			
Examples	-	ows how to configure a maximum number of addresses (5) on interface 1/1 for VLANs 2-3:		
	<pre>Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# interface g1/1 Switch(config-if)# switchport trunk encapsulation dot1q Switch(config-if)# switchport mode trunk Switch(config-if)# vlan 2-3 Switch(config-if-vlan-range)# port-security maximum 5 Switch(config-if-vlan-range)# exit Switch(config-if-vlan-range)# exit</pre>			

Related Commands	Command	Description
	port-security mac-address	Configures a secure address on an interface for a specific VLAN or VLAN range.
	port-security mac-address sticky	Configures a sticky address on an interface for a specific VLAN or VLAN range.

priority

To enable the strict priority queue (low-latency queueing [LLQ]) and to give priority to a class of traffic belonging to a policy map attached to a physical port, use the **priority** policy-map class configuration command. To return to the default setting, use the **no** form of this command.

priority

no priority

Syntax Description This command has no a	arguments or	keywords.
--	--------------	-----------

Defaults The strict priority queue is disabled.

Command Modes Policy-map class configuration

Command History Release Modification		Modification
	12.2(40)SG	This command was introduced on the Catalyst 4500 series switch using a
		Supervisor Engine 6E.

Usage Guidelines Use the **priority** command only in a policy map attached to a physical port. You can use this command only in class-level classes, you cannot use this command in class class-default.

This command configures LLQ and provides strict-priority queueing. Strict-priority queueing enables delay-sensitive data, such as voice, to be sent before packets in other queues are sent. The priority queue is serviced first until it is empty.

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

You can use police or set class configuration commands with the priority police-map class configuration command.

If the priority queuing class is not rate limited, you cannot use the bandwidth command, you can use the bandwidth remaining percent command instead.

Examples

This example shows how to enable the LLQ for the policy map called *policy1*:

Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# policy-map policy1 Switch(config-pmap)# class voice Switch(config-pmap-c)# priority

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

Γ

Related Commands

Command	Description	
bandwidth	Specifies or modifies the minimum bandwidth provided to a class belonging to a policy map attached to a physical port.	
class	Specifies the name of the class whose traffic policy you want to create or change.	
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.	
dbl	Enables dynamic buffer limiting for traffic hitting this class.	
service-policy (policy-map class)	Creates a service policy that is a quality of service (QoS) policy within a policy map.	
shape (class-based queueing)) Enables traffic shaping a class of traffic in a policy map attached to a physical port.	
show policy-map	Displays information about the policy map.	

private-vlan

	To configure private VLANs and the association between a private VLAN and a secondary VLAN, use the private-vlan command. To return to the default value, use the no form of this command.		
	private-vlan	{isolated community primary}	
	<pre>private-vlan association secondary-vlan-list [{add secondary-vlan-list} {remove secondary-vlan-list}] no private-vlan {isolated community primary}</pre>		
	no private-v	lan association	
Syntax Description	isolated	Designates the VLAN as an isolated private VLAN.	
	community	Designates the VLAN as the community private VLAN.	
	primary	Designates the VLAN as the primary private VLAN.	
	association	Creates an association between a secondary VLAN and a primary VLAN.	
	secondary-vlan-	<i>list</i> Specifies the number of the secondary VLAN.	
	add	(Optional) Associates a secondary VLAN to a primary VLAN.	
	remove	(Optional) Clears the association between a secondary VLAN and a primary VLAN.	
Defaults	Private VLANs a	re not configured.	
Command Modes	VLAN configuration mode		
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(20)EW	Support for community VLAN was added.	
Usage Guidelines	You cannot confi	gure VLAN 1 or VLANs 1001 to 1005 as private VLANs.	
	VTP does not support private VLANs. You must configure private VLANs on each device where you want private VLAN ports.		
	The <i>secondary_vlan_list</i> parameter cannot contain spaces; it can contain multiple comma-separated items. Each item can be a single private VLAN ID or a range of private VLAN 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 private VLAN 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 or by a community of ports to communicate with the switches.

An isolated VLAN is a VLAN that is used by the isolated ports to communicate with the promiscuous ports. The isolated VLAN traffic is blocked on all other private ports in the same VLAN and can be received only by the standard trunking ports and the promiscuous ports that are assigned to the corresponding primary VLAN.

A community VLAN is the VLAN that carries the traffic among the community ports and from the community ports to the promiscuous ports on the corresponding primary VLAN. A community VLAN is not allowed on a private VLAN trunk.

A promiscuous port is a private port that is assigned to a primary VLAN.

A primary VLAN is a VLAN that is used to convey the traffic from the switches to the customer end stations on the 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 that is 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 that are associated with the VLAN become inactive.

Refer to the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide* for additional configuration guidelines.

Examples

This example shows how to configure VLAN 202 as a primary VLAN and verify the configuration:

This example shows how to configure VLAN 303 as a community VLAN and verify the configuration:

This example shows how to configure VLAN 440 as an isolated VLAN and verify the configuration:

```
Switch# configure terminal
Switch(config)# vlan 440
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# end
```

Catalyst 4500 Series Switch Cisco IOS Command Reference—Release 12.2(46)SG

Switch#	show vlan	private-vlan
Primary	Secondary	Type Interfaces
202		primary
	303	community
	440	isolated
This ave	mpla chow	how to anote a private VI AN relationship among the primary VI AN

This example shows how to create a private VLAN 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 a private VLAN relationship and delete the primary VLAN. The associated secondary VLANs are not deleted.

```
Switch(config-vlan)# no private-vlan 14
Switch(config-vlan)#
```

This example shows how to associate community VLANs 303 through 307 and 309 and isolated VLAN 440 with primary VLAN 202 and verify the configuration:

```
Switch# configure terminal
Switch(config)# vlan 202
Switch(config-vlan)# private-vlan association 303-307,309,440
Switch(config-vlan)# end
Switch# show vlan private-vlan
```

Primary Secondary Type Interfaces _____ _____ 202 303 community 2.02 304 community 202 305 community 306 202 community 202 307 community 309 2.02 community 202 440 isolated 308 community



The secondary VLAN 308 has no associated primary VLAN.

This example shows how to remove an isolated VLAN from the private VLAN association:

```
Switch(config)# vlan 14
Switch(config-vlan)# private-vlan association remove 18
Switch(config-vlan)#
```

Administrative Mode: private-vlan host

This example shows how to configure interface FastEthernet 5/1 as a PVLAN host port and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 202 440
Switch(config-if)# end
Switch# show interfaces fastethernet 5/1 switchport
Name: Fa5/1
Switchport: Enabled
```

L

Operational Mode: private-vlan host Administrative Trunking Encapsulation: negotiate Operational Trunking Encapsulation: native Negotiation of Trunking: Off Access Mode VLAN: 1 (default) Trunking Native Mode VLAN: 1 (default) Voice VLAN: none Appliance trust: none Administrative Private Vlan Host Association: 202 (VLAN0202) 440 (VLAN0440) Promiscuous Mapping: none Trunk encapsulation : dot1q Trunk vlans: Operational private-vlan(s): 202 (VLAN0202) 440 (VLAN0440) Trunking VLANs Enabled: ALL Pruning VLANs Enabled: 2-1001 Capture Mode Disabled Capture VLANs Allowed: ALL

Related Commands	Command	Description	
	show vlan	Displays VLAN information.	
	show vlan private-vlan	Displays private VLAN information.	

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 this command.

private-vlan mapping primary-vlan-id {[secondary-vlan-list | {add secondary-vlan-list} |
 {remove secondary-vlan-list}]}

no private-vlan mapping

Syntax Description	primary-vlan-id	VLAN ID of the primary VLAN of the PVLAN relationship.
	secondary-vlan-list (Optional) VLAN ID of the secondary VLANs to map to the prim	
	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 mapping	s are removed.
Command Modes	Interface configuratio	on mode
Command History	Release Mo	odification
	12.1(8a)EW Su	pport for this command was introduced on the Catalyst 4500 series switch.
Usage Guidelines	2	<i>list</i> parameter cannot contain spaces. It can contain multiple, comma-separated be a single PVLAN ID or a range of PVLAN IDs separated by hyphens.
Usage Guidelines	items. Each item can	
Usage Guidelines	items. Each item can This command is vali	be a single PVLAN ID or a range of PVLAN IDs separated by hyphens.
Usage Guidelines	items. Each item can This command is vali The SVI of the prima	be a single PVLAN ID or a range of PVLAN IDs separated by hyphens. d in the interface configuration mode of the primary VLAN.
Usage Guidelines	items. Each item can This command is vali The SVI of the prima The traffic that is reco	be a single PVLAN ID or a range of PVLAN IDs separated by hyphens. d in the interface configuration mode of the primary VLAN. ry VLAN is created at Layer 3. eived on the secondary VLAN is routed by the SVI of the primary VLAN.
Usage Guidelines	items. Each item can This command is vali The SVI of the prima The traffic that is reco The SVIs of the existi is entered. A secondary SVI can different from what is	be a single PVLAN ID or a range of PVLAN IDs separated by hyphens. d in the interface configuration mode of the primary VLAN. ry VLAN is created at Layer 3.

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 the routing of the 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
isolated
vlan202 303
       304
vlan202
                     isolated
vlan202
        305
                     isolated
vlan202
        306
                     isolated
vlan202 307
                    isolated
vlan202 309
                    isolated
vlan202 440
                    isolated
Switch#
```

This example shows the displayed message that you will see if the VLAN that 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)#
```

```
Switch# configure 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
                      community
vlan202 304
                      community
vlan202 305
                      community
vlan202 306
                     community
vlan202 307
                     community
vlan202 309
                      community
vlan202 440
                      isolated
```

Switch#

Related Commands	Command	Description
	show interfaces private-vlan mapping	Displays PVLAN mapping information for VLAN SVIs.
	show vlan	Displays VLAN information.
	show vlan private-vlan	Displays private VLAN information.

private-vlan synchronize

To map the 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 the 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 sho	ows 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	Command	Description	
	show spanning-	tree mst Displays MST protocol information.	

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

Defaults	QoS functionality is disabled.
----------	--------------------------------

Command Modes Global configuration mode

 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 not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis. On the Supervisor Engine 6-E and Catalyst 4900M chassis QoS is always enabled without being configured.

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) # gos Switch(config) #

Related Commands	Command	Description
	qos (interface configuration mode)	Enables QoS functionality on an interface.
	show qos	Displays QoS information.

Γ

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 mode

 Release
 Modification

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

Usage Guidelines This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis. On the Supervisor Engine 6-E and Catalyst 4900M chassis, attaching a service policy implicitly enables QoS on the supervisor engine and detaching a service policy implicitly disables QoS on the supervisor engine.

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)# gos
 Switch(config-if)#

Related Commands	Command	Description	
	qos (global configuration mode)	Enables QoS functionality on the switch.	
	qos (interface configuration mode)	Enables QoS functionality on an interface.	
	show qos	Displays QoS information.	

Syntax Description

L

Oyntax Description	arpa	(18 bytes).
	dot1q	Specifies the account length of the 802.1Q-encapsulated packet (22 bytes).
	isl	Specifies the account length of the ISL-encapsulated packet (48 bytes).
	length len	Specifies the a dditional packet length to account for; the valid range is from 0 to 64 bytes.
Defaults	On man Sumamia	en Engine (Engels de langth that is angeified in the ID headen fan the ID mederte and
Delduits	-	sor Engine 6-Es only the length that is specified in the IP header for the IP packets and specified in the Ethernet header for non-IP packets are included.
		or Engine 6-E and Catalyst 4900M chassis the length that is specified in the Ethernet nto account for both IP and non-IP packets. The Layer 2 length includes the VLAN tag
Command Modes	Global configura	ation mode
Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Usage Guidelines	This command is	s not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.
	encapsulation c	500 series switch, for non-Superviosr Engine 6-E supervisors the qos account layer2 ommand indicates that the policing feature should consider the configured length in P length of the packet when policing the IP packets.
	Sharing and shap	ping always use the Ethernet ARPA length.
	Ethernet ARPA 1	ngine 6-E and Catalyst 4900M chassis supervisors shaping and sharing always use length to which 20 bytes of IPv6 overhead is always added for policing. However, only ncluding VLAN tag overhead is taken into account.
Note	it was received.	is included when policing all IP packets irrespective of the encapsulation with which When qos account layer2 encapsulation isl is configured, a fixed length of 48 bytes is olicing all IP packets, not only those IP packets that are received with ISL encapsulation.

Sharing and shaping use the length that is specified in the Layer 2 headers.

qos account layer2 encapsulation {arpa | dot1q | isl | length *len*}

no qos account layer2 encapsulation {arpa | dot1q | isl | length len}

To include additional bytes to be accounted by the QoS features, use the **qos account layer2 encapsulation** command. To disable the use of additional bytes, use the **no** form of this command.

Specifies the account length of the Ethernet ARPA-encapsulated packet

qos account layer2 encapsulation

arpa

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)# end Switch# This example shows how to disable the consistent accounting of the Layer 2 encapsulation by the QoS features: Switch# config terminal Switch(config)# no qos account layer2 encapsulation Switch(config)# no qos account layer2 encapsulation Switch (config)# end Switch

Related Commands	Command	Description
	show interfaces	Displays traffic on a specific interface.
	switchport	Modifies the switching characteristics of a Layer 2 switch interface.
	switchport block	Prevents the unknown multicast or unicast packets from being forwarded.

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	name	Name of the aggregate policer.		
	rate	Maximum bits per second; valid values are from 32000 to 3200000000.		
	burst	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 the QoS values are exceeded.		
	policed-dscp-transmit	(Optional) Sends the DSCP per the policed-DSCP map.		
Defaults	The default settings are a	The default settings are as follows:		
	Conform-action trans	smits		
	• Exceed-action drops			
Command History	Release Modifi	ication		
Command History		ication rt for this command was introduced on the Catalyst 4500 series switch.		
	12.1(8a)EW Suppo	rt for this command was introduced on the Catalyst 4500 series switch.		
	12.1(8a)EWSuppoThis command is not support	rt for this command was introduced on the Catalyst 4500 series switch. ported on the Supervisor Engine 6-E and Catalyst 4900M chassis.		
	12.1(8a)EWSuppoThis command is not supThis policer can be shared	rt for this command was introduced on the Catalyst 4500 series switch. ported on the Supervisor Engine 6-E and Catalyst 4900M chassis. d by different policy map classes and on different interfaces.		
Command History Usage Guidelines	12.1(8a)EWSuppoThis command is not supThis policer can be sharedThe Catalyst 4506 switch	ported on the Supervisor Engine 6-E and Catalyst 4900M chassis. d by different policy map classes and on different interfaces. a supports up to 1000 aggregate input policers and 1000 output policers.		
	12.1(8a)EWSupportThis command is not supportThis policer can be sharedThe Catalyst 4506 switchThe qos aggregate-policethat aggregate. When you	rt for this command was introduced on the Catalyst 4500 series switch. ported on the Supervisor Engine 6-E and Catalyst 4900M chassis. d by different policy map classes and on different interfaces.		

Suffix	Description
k	1000 bps
m	1,000,000 bps
g	1,000,000,000 bps

Rate Suffix

Bursts can be entered in bytes without a suffix. In addition, the suffixes shown in Table 2-11 are allowed.

Table 2-11 Burst Suffix

Table 2-10

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 that you configure might not be the value that is used.

Modifying an existing aggregate rate limit modifies that entry in NVRAM and 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.

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.

If you apply a single aggregate policer to the ports and the VLANs in different directions, then you have created the equivalent of four aggregate policers; one for all ports sharing the policer in the input direction, one for all ports sharing the policer in the output direction, one for all VLANs sharing the policer in the input direction.

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	Command	Description
	show qos aggregate policer	Displays QoS aggregate policer information.

qos control-packets

To enable Layer 2 control packet QoS mode on control packets use the **qos control-packets** command. To disable Layer 2 control packet QoS mode on control packets, use the **no** form of this command.

qos control-packets {bpdu-range | cdp-vtp | sstp}

no qos control-packets {bpdu-range | cdp-vtp | sstp}

Syntax Description	bpdu-range	Specifies enabling (OoS on BPDU-range packets.
	cdp-vtp	Specifies enabling (QoS on CDP and VTP packets.
	sstp	Specifies enabling (QoS on SSTP packets.
Defaults	This command	has no default settings.	
Command Modes	Global configur	ation mode	
Command History	Release	Modification	
	12.2(40)SG	Support for this command w	as introduced on the Catalyst 4500 series switch.
Usage Guidelines			
Usage Guidelines	This command	is not supported on the Supervis	or Engine 6-E and Catalyst 4900M chassis.
Usage Guidelines		ddresses that Layer 2 control pa	
Jsage Guidelines	The ranges of a	ddresses that Layer 2 control pa	cket QoS acts on when the relative command is entered
Jsage Guidelines	The ranges of a is shown in Tab Table 2-12	ddresses that Layer 2 control pa le 2-12:	cket QoS acts on when the relative command is entered
Usage Guidelines	The ranges of a is shown in Tab Table 2-12	ddresses that Layer 2 control pa le 2-12: Packet Type and Actionable Ac	cket QoS acts on when the relative command is entered
Jsage Guidelines	The ranges of a is shown in Tab <i>Table 2-12</i> Type of Packet	ddresses that Layer 2 control pa le 2-12: Packet Type and Actionable Ac	cket QoS acts on when the relative command is entered datess Range Range of address 0180.C200.0000 BPDU 0180.C200.0002 OAM, LACP

When Layer 2 control packet QoS is enabled, you need to configure policies to match the required Layer 2 packets and police them as desired. When the feature is enabled on a particular packet type, MACLs that match the desired control packets are automatically generated, if not already present. The corresponding class maps matching these MACLs are auto-generated as well. You can then use these class maps in the policy maps in order to police the control packets, applying them a per port, per VLAN, or per port per VLAN just like any other policy map. In addition, you can define your own MACLs/class maps to match the control packets. The only limitation is that the user-defined class maps have to begin with the prefix "system-control-packet-".

Examples

This example shows how to enable QoS on BDPU packets.

```
Switch#enable
Switch#configuration terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#gos control-packets bpdu-range
Switch(config)#
```

This example shows how to enable QoS on CDP and VTP packets.

```
Switch#enable
Switch#configuration terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#gos control-packets cdp-vtp
Switch(config)#
```

This example shows how to enable QoS on SSTP packets.

```
Switch#enable
Switch#configuration terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#gos control-packets sstp
Switch(config)#
```

Related Commands	Command	Description
	show policy-map interface	Displays the statistics and configurations of the input and output policies that are attached to an interface.
	show running-config	Displays the running-configuration for a switch.

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	cos_value	Default CoS value for the interface; valid values are from 0 to 7.
Defaults	-	isor Engine 6-E supervisors the default CoS value is 0. Engine 6-E and Catalyst 4900M chassis supervisors the default CoS is implicitly set to 1.
<u>Note</u>	CoS override is	not configured.
Command Modes	Interface config	guration mode
Command History	Release 12.1(8a)EW	Modification Support for this command was introduced on the Catalyst 4500 series switch.
Usage Guidelines		is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis. configurable on physical LAN ports only.
Examples	-	hows how to configure the default QoS CoS value as 6: -if)# gos cos 6 -if)#
Related Commands	Command show gos	Description Displays QoS information.

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} | dscp-based {value | value range} | exceed-action {ecn | probability
 percent} | flow {include [layer4-ports] [vlan]}]
- no qos dbl [buffers {aggressive-flow buffers} | credits {aggressive-flow credits |
 maximum max} | dscp-based {value | value range} | exceed-action {ecn | probability
 percent} | flow {include [layer4-ports] [vlan]}]

Syntax Description	buffers	(Optional) Specifies the buffer limit for aggressive flows.
	aggressive-flow	(Optional) Specifies the aggressive flow.
	buffers	(Optional) Number of buffers for aggressive flows; valid values are from 0 to 255.
	credits	(Optional) Specifies the credit limit for aggressive flows and all flows.
	credits	(Optional) Number of credits for aggressive flows; valid values are from 0 to 15.
	maximum	(Optional) Specifies the maximum credit for all flows.
	max	(Optional) Number of credits for all flows; valid values are from 0 to 15.
	dscp-based	(Optional) Specifies the packets that belong to the list of internal DSCPs.
	value	(Optional) A single DSCP value; valid values are from 0 to 63.
	value range	(Optional) A range of DSCP values; valid values are from 0 to 63. Up to 8 command separated DSCP values can be specified.
	exceed-action	(Optional) Specifies the packet marking when the limits are exceeded.
	ecn	(Optional) Specifies the explicit congestion notification.
	probability	(Optional) Specifies the probability of packet marking.
	percent	(Optional) Probability number; valid values are from 0 to 100.
	flow	(Optional) Specifies the flows for limiting.
	include	(Optional) Allows the Layer 4 ports and VLANs to be included in the flows.
	layer4-ports	(Optional) Includes the Layer 4 ports in flows.
	vlan	(Optional) Includes the VLANs in flows.

Defaults

On non-Supervisor Engine 6-E supervisors the default settings are as follows:

- QoS DBL is disabled.
- Aggressive-flow buffers is set to 2.
- Aggressive-flow credits is set to 2, with a limit of 10.
- Layer 4 ports are included.
- VLANs are included.
- 15 maximum credits are allowed.
- 15% drop probability is set.
- DSCP values are included.

On Supervisor Engine 6-E and Catalyst 4900M chassis supervisors the default dbl values are implicitly set and cannot be changed. The settings are as follows:

- seven maximum credits allowed.
- Aggressive-flow credits is set to 4.
- Aggressive-flow buffers is set to 4.
- six percent drop probability is set.
- Hash function for Layer 2 packets uses source and destination MAC addresses as well as transmit VLAN identifiers.
- Hash function for IPv4 and IPv6 packets uses source and destination IP addresses source and destination Layer 4 ports as well as transmit VLAN identifiers.

 Command Modes
 Global configuration mode

 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.
	12.2(37)SG	Added support for DSCP-based flow management.

Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.

Examples

This example shows how to enable DBL globally on the switch:

Switch(config)# **gos dbl** 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-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# dbl
Switch(config-pmap-c)#
```

This example shows how to selectively enable DBL on DSCP values 1 through 10:

```
Switch# configure t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# qos dbl dscp-based 1-10
Switch(config)# end
Switch# show qos dbl
DBL flow includes vlan
DBL flow includes layer4-ports
DBL does not use ecn to indicate congestion
DBL exceed-action probability: 15%
DBL max credits: 15
DBL aggressive credit limit: 10
DBL aggressive buffer limit: 2 packets
DBL DSCPs with default drop probability:
```

1-10

This example shows how to selectively disable DBL on DSCP values 1 through 10:

```
Switch# configure t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# no qos dbl dscp-based 1-5, 7
Switch(config)# end
Switch# show qos dbl
DBL flow includes vlan
DBL flow includes layer4-ports
DBL does not use ecn to indicate congestion DBL exceed-action probability: 15% DBL max
credits: 15 DBL aggressive credit limit: 10 DBL aggressive buffer limit: 2 packets DBL
DSCPs with default drop probability:
0,6,8-63
```

You can verify your settings by entering the show qos dbl privileged EXEC command.

Related Commands	Command	Description				
	show qos dbl	Displays QoS Dynamic Buffer Limiting (DBL) information.				

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	dscp_value	Default DSCP value for the interface; valid values are from 0 to 63.		
Defaults	On non-Supervi	isor Engine 6-E supervisors the default DSCP value is 0.		
	On Supervisor I to 0.	Engine 6-E and Catalyst 4900M chassis supervisors the port DSCP value is always set		
Command Modes	Interface config	guration mode		
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 not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.		
Examples	This example shows how to configure the default QoS DSCP value as 6:			
	Switch(config- Switch(config-	-if)# qos dscp 6 -if)#		
Related Commands	Command	Description		
	show qos inter	face Displays QoS information for an interface.		

qos map cos

To define the ingress CoS-to-DSCP mapping for the trusted interfaces, use the **qos map cos to dscp** command. To remove a prior entry, use the **no** form of this command.

Note

You cannot remove a single entry from the table.

qos map cos cos_values to dscp dscp1

no qos map cos to dscp

Syntax Description	cos_values	CoS values; list up to eight CoS values separated by spaces.
	to dscp	Defines mapping and specifies DSCP value.
	dscp1	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 configuratio	n mode
--	--------

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 not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis. In place of this limited map capability, the Supervisor Engine 6-E and Catalyst 4900M chassis supports the setting of various marking fields in a packet within a policy map. Please refer to the **set** command for more details.

The CoS-to-DSCP map is used to map the packet CoS (on the interfaces that are 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 values. 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 clear the entire CoS-to-DSCP mapping table:				
	Switch(config)# no gos map cos 0 to dscp 20				

Switch(config)#

Related Commands

ommands	Command	Description		
	qos map dscp	Maps the DSCP values to selected transmit queues and to map the DSCP-to-CoS value.		
	qos map dscp policed	Sets the mapping of the policed DSCP values to the marked-down DSCP values.		
	show qos	Displays QoS information.		
	tablemap (refer to Cisco IOS documentation)	Modifies metric and tag values when the IP routing table is updated with BGP learned routes.		
qos map dscp

To map the 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	dscp-ve	alues				s to map	to the c	queue II); valid	values are from 0 to 63.
	to		Defines mapping.							
		tx-queueSpecifies a transmit queue.								
	queue-									
	cos		-		e CoS v					
	cos-va	lue	Clas	ss of ser	vice; va	lid value	es are fr	om 1 to	7.	
Defaults	The def	fault D	SCP-to	-CoS co	onfigura	tion sett	ings are	shown	in the fo	llowing 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	-
	000	0	1	2	5	-	5	0	/	
Command History	Releas			odificat		<u></u>		traduca	d on the	Cotalust 4500 sories switch
	12.1(8	a)Ew	5	ipport f	or this c	ommand	1 was in	troduce	a on the	Catalyst 4500 series switch.
Usage Guidelines										
	this cor	nmano	l the Su	perviso		6-E and	d Cataly	st 4900	M chassi	atalyst 4900M chassis. In place of s uses the tablemap command for
	this cor QoS ma You use written table of	nmano arking e the I into the f 64 D	l the Su . Please DSCP-to he ISL I SCP vai	perviso: refer to -CoS m neader o	r Engine the tab tap to m or 802.10	• 6-E and elemap of ap the fi Q tag of respondi	d Cataly comman inal DSC the tran ing CoS	st 4900 d for de CP class smitted values.	M chassi tails. ification packet o	• •
	this cor QoS ma You use written table of to eight The DS	nmand arking e the I into the f 64 D t DSC CP-to	l the Su . Please DSCP-to he ISL l SCP va P values -transm	perviso refer to p-CoS m neader o lues and s, separa it-queu	r Engine o the tab nap to m or 802.10 the corr ated by s e map is	e 6-E and elemap of ap the fi Q tag of respondi- spaces, f used to	d Cataly comman inal DSC the tran ing CoS for a Cos map the	st 4900 d for de CP class smitted values. S value. final D	M chassi tails. ification packet o The swi	s uses the tablemap command for to a final CoS. The CoS map is on trunk interfaces and contains a
Examples	this cor QoS ma You use written table of to eight The DS can ent	nmano arking e the I into the f 64 D t DSC GCP-to er up t	l the Su . Please DSCP-to he ISL l SCP va P values -transm o eight	perviso refer to p-CoS m header o lues and s, separa it-queue DSCP	r Engine o the tab nap to m or 802.10 the corr ated by s e map is	e 6-E and olemap of ap the fi Q tag of respondi spaces, f used to eparated	d Cataly comman inal DSC the tran ing CoS for a CoS map the d by spa	st 4900 d for de CP class smitted values. S value. final D ces, for	M chassi tails. ification packet o The swi SCP clas a transm	s uses the tablemap command for to a final CoS. The CoS map is on trunk interfaces and contains a tch has one map. You can enter up sification to a transmit queue. You it queue.

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	Command	Description	
	qos map cos	Defines the ingress CoS-to-DSCP mapping for the trusted interfaces.	
	show qos interface	Displays queueing information.	
	show qos	Displays QoS information.	
	tablemap (refer to Cisco IOS documentation)	Modifies metric and tag values when the IP routing table is updated with BGP learned routes.	
	tx-queue	Configures the transmit queue parameters for an interface.	

Catalyst 4500 Series Switch Cisco IOS Command Reference—Release 12.2(46)SG

qos map dscp policed

To set the mapping of the policed DSCP values to the 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	dscp_list	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 DSC	CP values is disabled.				
Command Modes	Global configura	ation mode				
Command History	Release	Modification				
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.				
Usage Guidelines	policer types are explicit QoS ma The DSCP-to-po out-of-profile flo	s not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis. Various e supported on the Supervisor Engine 6-E and Catalyst 4900M chassis that supports rking of DSCP, precedence, and CoS fields. Refer to the police command for details. oliced-DSCP map determines the marked-down DSCP value that is applied to the pows. The switch has one map.				
	You can enter up to eight DSCP values, separated by spaces.					
•	You can enter of	nly one policed DSCP value.				
<u>Note</u>		sequence packets, configure the DSCP-to-policed-DSCP map so that marked-down n the same queue as in-profile traffic.				
Examples	-	ows how to map multiple DSCPs to a single policed-DSCP value: # gos map dscp policed 20 25 43 to dscp 4 #				

Related Commands	Command	Description
	qos map cos	Defines the ingress CoS-to-DSCP mapping for the trusted interfaces.
	qos map dscp	Maps the DSCP values to selected transmit queues and to map the DSCP-to-CoS value.
	show qos	Displays QoS information.

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 this command.

qos rewrite ip dscp

no qos rewrite ip dscp

Syntax Description	This command has no argun	nents or keywords.
--------------------	---------------------------	--------------------

Defaults	IP DSCP rewrite is enabled.
----------	-----------------------------

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 This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.

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 This example shows how to disable IP DSCP rewrite: Switch(config) # no gos rewrite ip dscp Switch(config) #

Related Commands	Command	Description	
	qos (global configuration mode)	Enables QoS functionality on the switch.	
	show qos	Displays QoS information.	

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.			
	device cisco-phon	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 to extend the trust to Port VLAN ID (PVID) packets coming from the PC.			
	cos priority	(Optional) Specifies that the CoS priority value is set to PVID packets; valid values are from 0 to 7.			
Defaults	The default setting	zs are as follows:			
	-	is enabled, trust is disabled on the port.			
	-	is disabled, trust DSCP is enabled on the port.			
	•	-			
	• The CoS prior	rity level is 0.			
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 was added.			
Jsage Guidelines	This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.				
	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).				
	the default CoS fo When the interface				

Trusted boundary should not be configured on the ports that are part of an EtherChannel (that is, a port channel).

ExamplesThis example shows how to set the trusted state of an interface to CoS:
Switch(config-if)# gos trust cos
Switch(config-if)#This example shows how to set the trusted state of an interface to DSCP:
Switch(config-if)# gos trust dscp
Switch(config-if)#This example shows how to set the PVID CoS level to 6:
Switch(config-if)#Switch(config-if)#
Switch(config-if)#This example shows how to set the PVID CoS level to 6:
Switch(config-if)#Switch(config-if)#
This example shows how to set the Cisco phone as the trust device:
Switch(config-if)#Switch(config-if)#
Switch(config-if)#This example shows how to set the Cisco phone
Switch(config-if)#

Related Commands	Command	Description	
	qos cos	Defines the default CoS value for an interface.	
	qos vlan-based	Defines per-VLAN QoS for a Layer 2 interface.	
	show qos interface	Displays QoS information for an 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 mode

 Release
 Modification

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

Usage Guidelines This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis. On the Supervisor Engine 6-E and Catalyst 4900M chassis various QoS marking and policing actions at the interface and VLAN level are appropriately merged. For details, refer to the *Catalyst 4500 Series Switch Configuration Guide*.

In VLAN-based mode, the policy map that is attached to the Layer 2 interface is ignored, and QoS is driven by the policy map that is attached to the corresponding VLAN interface.

Per-VLAN QoS can be configured only on the Layer 2 interfaces.

If no input QoS policy is attached to a Layer 2 interface, then the input QoS policy that is 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 that is 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 mode.

Examples

This example shows how to enable per-VLAN QoS for a Layer 2 interface:

Switch(config-if)# gos vlan-based
Switch(config-if)#

Related Commands	Command	Description
	qos cos	Defines the default CoS value for an interface.
	show qos interface	Displays QoS information for an interface.

queue-limit

To specify or modify the maximum number of packets the queue can hold for a class policy configured in a policy map, use the **queue-limit** command. To remove the queue packet limit from a class, use the **no** form of this command.

queue-limit number-of-packets

no queue-limit number-of-packets

Syntax Description	number-of-packets	Number of packets that the queue for this class can accumulate; valid range is 16 to 8184. This number must be a multiple of 8.		
Defaults		cal interface on a Catalyst 4500 switch has a default queue based on the number d the number of ports on the linecards.		
Command Modes	QoS policy-map class	configuration mode		
Command History	Release	Modification		
	12.2(44)SG	This command was introduced on the Catalyst 4500 series switch.		
Usage Guidelines	This class-based queuin on the Catalyst 4500 st	ng (CBQ) command applies only to the Supervisor 6E as part of the MQC support upervisor.		
	of this queue is based of in each slot. The switch pool. The remaining 4	cal interface on a Catalyst 4500 switch comes up with a default queue. The size on the number of slots in a chassis as well as the number of ports on the line card a supports 512K queue entries of which 100K are set aside as a common sharable 12K entries are equally distributed among the slots. Each slot further divides its a equally among its ports.		
	CBQ creates a queue for every class for which a class map is defined. Packets satisfying the match criterion for a class accumulate in the queue reserved for the class until they are sent, which occurs when the queue is serviced by the fair queuing process. When the maximum packet threshold you defined for the class is reached, queuing of any further packets to the class queue causes tail drop or, if DBL is configured for the class policy, packet drop to take effect.			
<u>Note</u>		and is supported only after you first configure a scheduling action, such as riority, except when you configure queue-limit in the class-default class of an		

output QoS policy-map.s

Examples

This example shows how to configure a policy-map called *policy11* to contain policy for a class called *acl203*. Policy for this class is set so that the queue reserved for it has a maximum packet limit of 40:

```
Switch# configure terminal
Switch (config)# policy-map policy11
Switch (config-pmap)# class acl203
Switch (config-pmap-c)# bandwidth 2000
Switch (config-pmap-c)# queue-limit 40
Switch (config-pmap-c)# end
Switch#
```

Related Commands	Command	Description
	bandwidth	Specifies or modifies the minimum bandwidth provided to a class belonging to a policy map attached to a physical port.
	class	Specifies the name of the class whose traffic policy you want to create or change.
	policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
	shape (class-based queueing)	Enables traffic shaping a class of traffic in a policy map attached to a physical port.

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 mode

 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 reenable 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-red)#

This example shows how to enter the main CPU submode:

Switch(config)# redundancy
Switch(config-red)# main-cpu
Switch(config-r-mc)#

Related Commands	Command	Description
	auto-sync	Enables automatic synchronization of the configuration files in NVRAM.
	main-cpu	Enters the main CPU submode and manually synchronize the configurations on the two supervisor engines.

redundancy config-sync mismatched-commands

If your active and standby supervisors are running different versions of IOS, some of their CLIs will not be compatible. If such commands are already present in the running configuration of the active supervisor engine and the syntax-check for the command fails at the standby supervisor engine while it is booting, the **redundancy config-sync mismatched-commands** command moves the active supervisor engine into the Mismatched Command List (MCL) and resets the standby supervisor engine.

redundancy config-sync {ignore | validate} mismatched-commands

	ignore	Ignore the mismatched command list.	
	validate	Revalidate the mismatched command list with the modified running-configuration.	
Defaults	This command has	no default settings.	
Command Modes	Privileged EXEC m	Privileged EXEC mode	
Command History	Release	Modification	
	12.2(31)SGA	This command was introduced on the Catalyst 4500 series switch.	
	12.2(44)SG	Updated command syntax from issu config-sync to redundancy config-sync.	
Usage Guidelines	The following is a l	og entry example for mismatched commands:	
Usage Guidelines	00:06:31: Config full list of mism	og entry example for mismatched commands: Sync: Bulk-sync failure due to Servicing Incompatibility. Please check atched commands via: config-sync failures mcl	
Usage Guidelines	00:06:31: Config full list of mism show redundancy 00:06:31: Config	Sync: Bulk-sync failure due to Servicing Incompatibility. Please check atched commands via: config-sync failures mcl Sync: Starting lines from MCL file:	
Usage Guidelines	00:06:31: Config full list of mism show redundancy	Sync: Bulk-sync failure due to Servicing Incompatibility. Please check atched commands via: config-sync failures mcl Sync: Starting lines from MCL file: Ethernet7/7 erface" .0.1 255.0.0.0	
Usage Guidelines	00:06:31: Config full list of mism show redundancy 00:06:31: Config interface Gigabit ! <submode> "int - ip address 11.0 ! </submode> "in	Sync: Bulk-sync failure due to Servicing Incompatibility. Please check atched commands via: config-sync failures mcl Sync: Starting lines from MCL file: Ethernet7/7 erface" .0.1 255.0.0.0	
Usage Guidelines	00:06:31: Config full list of mism show redundancy 00:06:31: Config interface Gigabit ! <submode> "int - ip address 11.0 ! </submode> "in	Sync: Bulk-sync failure due to Servicing Incompatibility. Please check atched commands via: config-sync failures mcl Sync: Starting lines from MCL file: Ethernet7/7 erface" .0.1 255.0.0.0 terface" matched commands, use the show redundancy config-sync failures mcl command.	
Usage Guidelines Step 1	00:06:31: Config full list of mism show redundancy 00:06:31: Config interface Gigabit ! <submode> "int - ip address 11.0 ! </submode> "in To display all mism To clean the MCL,	Sync: Bulk-sync failure due to Servicing Incompatibility. Please check atched commands via: config-sync failures mcl Sync: Starting lines from MCL file: Ethernet7/7 erface" .0.1 255.0.0.0 terface" matched commands, use the show redundancy config-sync failures mcl command.	
	00:06:31: Config full list of mism show redundancy 00:06:31: Config interface Gigabit ! <submode> "int - ip address 11.0 ! </submode> "in To display all mism To clean the MCL, f Remove all mismate Revalidate the MCI	Sync: Bulk-sync failure due to Servicing Incompatibility. Please check atched commands via: config-sync failures mcl Sync: Starting lines from MCL file: Ethernet7/7 erface" .0.1 255.0.0.0 terface" watched commands, use the show redundancy config-sync failures mcl command. follow these steps:	

You could also ignore the MCL	by doing	the following:
-------------------------------	----------	----------------

- Step 1 Enter the redundancy config-sync ignore mismatched-commands command.
- Step 2 Reload the standby supervisor engine; the system changes to SSO mode.
 - Note If you ignore the mismatched commands, the *out-of-sync* configuration at the active supervisor engine and the standby supervisor engine still exists.
- Step 3 You can verify the ignored MCL with the show redundancy config-sync ignored mcl command.

Examples	This example shows how you can validate removal of entries from the MCL:		
	Switch# redundancy config-syr Switch#	nc validate mismatched-commands	
Related Commands	Command	Description	

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)EWSupport for this command was introduced on the Catalyst 4500 series switch
(Catalyst 4507R only).

Usage GuidelinesBefore using this command, refer to the "Performing a Software Upgrade" section of the Catalyst 4500
Series Switch Cisco IOS 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 Cisco IOS 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	Command	Description	
	redundancy	Enters the redundancy configuration mode.	
	show redundancy	Displays redundancy facility information.	

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 h	nas 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	-	s command, refer to the "Performing a Software Upgrade" section of the <i>Catalyst 4500</i> isco IOS Software Configuration Guide for additional information.
	The redundanc reset.	y reload shelf command conducts a reboot of both supervisor engines. The modules are
Examples	This example sh	nows how to manually reload one or both supervisor engines:
	Switch# redund Switch#	ancy reload shelf
Related Commands	Command	Description
	redundancy	Enters the redundancy configuration mode.

Displays redundancy facility information.

remote login module

To remotely connect to a specific module, use the remote login module configuration command.

remote login module mod

Syntax Description	mod Target	module for the command.	
Defaults	This command has	no default settings.	
Command Modes	Privileged		
Command History	Release	Modification	
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.	
Usage Guidelines	This command applies only to the Access Gateway Module on Catalyst 4500 series swi The valid values for <i>mod</i> depends on the chassis used. For example, if you have a Catalys		
		module are from 2 to 6. If you have a 4507R chassis, valid values are from 3 to 7.	
	•	he remote login module <i>mod</i> command, the prompt changes to Gateway#	
	The remote login n commands.	nodule command is identical to the session module <i>mod</i> and the attach module <i>mod</i>	
Examples	This example show	s 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	Command	Description	
	attach module	Remotely connects to a specific module.	
	session module	Logs in to the standby supervisor engine using a virtual console.	

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 mode

 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	Command	Description
	monitor session	Enables the SPAN sessions on interfaces or VLANs.

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) Specifie	s that the checksum associated with the contents of the file	
Oyntax Description	vanuation none	specified by the Ul		
	url	(Optional) Specifie	s the file from which the read is performed.	
Defaults	This command ha	as no default settings.		
Command Modes	Privileged EXEC	Privileged EXEC mode		
Command History	Release	Modification		
	12.1(19)EW	Support for this comm	and was introduced on the Catalyst 4500 series switch.	
Usage Guidelines	If the URL is not	provided, the switch trie	es to read the file from the configured URL.	
Examples	This example sho	ws how to renew the DI	ICP binding database while bypassing the CRC checks:	
			0 1 0	
	Switch# renew i) Switch#	p dhcp snooping datab		
Related Commands		p dhcp snooping datab		
Related Commands	Switch#		ase validation none	
Related Commands	switch#	g	ase validation none Description	
Related Commands	Switch# Command ip dhcp snoopin ip dhcp snoopin	g	Description Globally enables DHCP snooping. Sets up and generates a DHCP binding configuration to	
Related Commands	Switch# Command ip dhcp snoopin ip dhcp snoopin	g g binding g information option	Description Globally enables DHCP snooping. Sets up and generates a DHCP binding configuration to restore bindings across reboots.	
Related Commands	Switch# Command ip dhcp snoopin ip dhcp snoopin ip dhcp snoopin	g g binding g information option g trust	Description Globally enables DHCP snooping. Sets up and generates a DHCP binding configuration to restore bindings across reboots. Enables DHCP option 82 data insertion.	
Related Commands	Switch# Command ip dhcp snoopin ip dhcp snoopin ip dhcp snoopin ip dhcp snoopin	g g binding g information option g trust g vlan	Description Globally enables DHCP snooping. Sets up and generates a DHCP binding configuration to restore bindings across reboots. Enables DHCP option 82 data insertion. Enables DHCP snooping on a trusted VLAN.	

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 mode

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 reset the proposed new VLAN database 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	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		
<u> </u>	Be careful when u	hey are considered to be part of two different regions. ing the revision command to set the MST configuration revision number because switch in a different region.		
Examples	This example show	s how to set the configuration revision number:		
	Switch(config-ms			
Related Commands	Command	Description		
	instance	Maps a VLAN or a set of VLANs to an MST instance.		
	name	Sets the MST region name.		
	show spanning-ti	ee mst Displays MST protocol information.		

Enters the MST configuration submode.

spanning-tree mst configuration

service-policy (interface configuration)

To attach a policy map to an interface or to apply different QoS policies on VLANs that an interface belongs to, 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 the input policy maps.	
	output	Specifies the output policy maps.	
	policy-map name	Name of a previously configured policy map.	
Defaults	A policy map is no	ot attached to an interface or a VLAN.	
Command Modes	Interface configura	ition mode	
Command History	Release	Modification	
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.	
	12.2(25)EWA	Support for applying different QoS policies on VLANs was introduced.	
Note	different VLANs.	nmand, you can use the service-policy command to specify different QoS policies on restricted to Layer 2 interfaces.	
Note		estituted to Edyor 2 Interfaces.	
	Non-Supervisor Eng	ine 6-E	
	You cannot apply a policy map under an interface and a VLAN range at the same time.		
	To attach a service policy to a VLAN an SVI must be created for the VLAN and the applied to the SVI.		
	Supervisor Engine 6-E and Catalyst 4900M chassis		
	this is allowed only	rvice policy under an interface as well as a VLAN range at the same time. However, y when the interface policy has only queuing actions whereas a VLAN has only ons (QoS marking and/or policing) actions.	
	To attach a service	policy to a VLAN, the VLAN configuration mode has to be used.	

To attach a service policy to a VLAN, the VLAN configuration mode has to be used.

```
Examples
                    This example shows how to attach a policy map to Fast Ethernet interface 5/20:
                    Switch# configure terminal
                   Enter configuration commands, one per line. End with CNTL/Z.
                   Switch(config)# interface fastethernet 5/20
                   Switch(config-if)# service-policy input pmap1
                    Switch(config-if)# end
                   This example shows how to apply policy map p1 for traffic in VLANs 20 and 400, and policy map p2
                   for traffic in VLANs 300 through 301:
                   Switch# configure terminal
                   Switch(config)# interface gigabitEthernet 6/1
                   Switch(config-if)# switchport trunk encapsulation dot1q
                   Switch(config-if)# switchport mode trunk
                   Switch(config-if)# vlan-range 20,400
                   Switch(config-if-vlan-range)# service-policy input p1
                   Switch(config-if-vlan-range)# exit
                   Switch(config-if)# vlan-range 300-301
                   Switch(config-if-vlan-range)# service-policy output p2
                   Switch(config-if-vlan-range)# end
                   Switch# show policy-map interface gigabitEthernet 6/1 vlan 20
                    GigabitEthernet6/1 vlan 20
                      Service-policy input: p1
                        Class-map: class-default (match-any)
                          0 packets
                          Match: any
                            0 packets
                          police: Per-interface
                            Conform: 0 bytes Exceed: 0 bytes
                   Switch# show policy-map interface gigabitEthernet 6/1
                    GigabitEthernet6/1 vlan 20
                      Service-policy input: p1
                        Class-map: class-default (match-any)
                          0 packets
                          Match: any
                            0 packets
                          police: Per-interface
                            Conform: 0 bytes Exceed: 0 bytes
                     GigabitEthernet6/1 vlan 300
                      Service-policy output: p2
                        Class-map: class-default (match-any)
                          0 packets
                          Match: any
                            0 packets
                          police: Per-interface
                            Conform: 0 bytes Exceed: 0 bytes
                     GigabitEthernet6/1 vlan 301
                      Service-policy output: p2
                        Class-map: class-default (match-any)
                          0 packets
                          Match: any
                            0 packets
```

```
police: Per-interface
Conform: 0 bytes Exceed: 0 bytes
GigabitEthernet6/1 vlan 400
Service-policy input: p1
Class-map: class-default (match-any)
0 packets
Match: any
0 packets
police: Per-interface
Conform: 0 bytes Exceed: 0 bytes
```

This example shows how to attach a policy map to a VLAN using an SVI on a non-Supervisor Engine 6-E:

```
Switch# configure terminal
Switch(config)#interface vlan 10
Switch(config-if)#service-policy out policy-vlan
Switch(config-if)#end
Switch#
```

This example shows how to attach a policy map to a VLAN using a Supervisor Engine 6-E:

```
Switch# configure terminal
Switch(config)#vlan configuration 20
Switch(config-vlan-config)#service-policy out policy-vlan
Switch(config-vlan-config)#end
Switch#
```

Related Commands	Command	Description
	class-map	Creates a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode.
	policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
	service-policy (interface configuration)	Attaches a policy map to an interface.
	show policy-map interface vlan	Displays the QoS policy-map information applied to a specific VLAN on an interface.

service-policy (policy-map class)

To create a service policy that is a quality of service (QoS) policy within a policy map (called a hierarchical service policy), use the **service-policy** policy-map class configuration command. To disable the service policy within a policy map, use the **no** form of this command.

service-policy policy-map-name

no service-policy policy-map-name

Syntax Description	policy-map-name	Name of the policy map.	
Defaults	No service policies maps are defined.		
Command Modes	Policy-map class co	onfiguration	
Command History	Release	Modification	
-	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.	
	12.2(40)SG	Added support for Supervisor Engine 6-E and Catalyst 4900M chassis.	
	having the child policy map specify the queueing actions. If you enter this command in policy-map class configuration mode, you return to policy-map configuration mode by using the exit command. To return to privileged EXEC mode, use the end command.		
Examples	command.		
		settings by entering the show policy-map privileged EXEC command.	

Related Commands	Command	Description
	bandwidth	Creates a signaling class structure that can be referred to by its name.
	class	Specifies the name of the class whose traffic policy you want to create or change.
	dbl	Enables active queue management on a transmit queue used by a class of traffic.
	policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
	priority	Enables the strict priority queue (low-latency queueing [LLQ]) and to give priority to a class of traffic belonging to a policy map attached to a physical port.
	random-detect (refer to Cisco IOS documentation)	Enables Weighted Random Early Detection (WRED) or distributed WRED (DWRED).
	shape (class-based queueing)	Enables traffic shaping a class of traffic in a policy map attached to a physical port.
	show policy-map	Displays information about the policy map.

service-policy input (control-plane)

To attach a policy map to a control plane for aggregate control plane services, use the **service-policy input** command. Use the **no** form of this command to remove a service policy from a control plane.

service-policy input policy-map-name

Syntax Description	input	Applies the specified service policy to the packets that are entering the control plane.
	policy-map-name	Name of a service policy map (created using the policy-map command) to be attached.
Defaults	No service policy is s	pecified.
Command Modes	Control-plane configu	iration
Command History	Release	Modification
	12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switch.
	 the global macro system-cpp command to attach it to the control-plane. The system-cpp-policy created by the system contains system pre-defined classes. For these pre-defined classes, you can change the policing parameters but you should not make any other change to the classes. You can define your own class-maps and append them to the end of the system-cpp-policy policy-map. 	
Examples	-	now to configure trusted hosts with source addresses 10.1.1.1 and 10.1.1.2 to ts to the control plane without constraint, while allowing all remaining Telnet at the specified rate:
	<pre>! Allow 10.1.1.2 tr Switch(config)# acc ! Rate limit all ot Switch(config)# acc ! Define class-map</pre>	
	Switch(config-cmap) Switch(config-cmap) Switch(config) # pol	uss-map telnet-class # match access-group 140 # exit .icy-map control-plane-policy # class telnet-class
	Switch(config-pmap- Switch(config-pmap- Switch(config-pmap)	c)# police 80000 conform transmit exceed drop

Switch(config)# control-plane
Switch(config-cp)# service-policy input control-plane-policy
Switch(config-cp)# exit

Related Commands	Command	Description
	control-plane	Enters control-plane configuration mode.
	macro global apply system-cpp	Applies the control plane policing default template to the switch.
	policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
	show policy-map control-plane	Displays the configuration either of a class or of all classes for the policy map of a control plane.

session module

Note	This command is only supported in SSO mode and does not work in RPR mode. To login to the standby supervisor engine using a virtual console, 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		
	12.2(31)SGSupport for this command was introduced on the Catalyst 4500 series switch		
Usage Guidelines	Catalyst 4500 series switches can be configured with 2 supervisor engines to provide redundancy. Whe the switch is powered, one of the supervisor engines becomes active and remains active until a switchover occurs. The other supervisor engine remains in standby mode.		
	Each supervisor engine has its own console port. Access to the standby supervisor engine is possible only through the console port of the standby supervisor engine. Therefore, you must connect to the standby console to access, monitor or debug the standby supervisor.		
	Virtual Console for Standby Supervisor Engine enables you to access the standby console from the activ supervisor engine without requiring a physical connection to the standby console. It uses IPC over EOBC to communicate with the standby supervisor engine and thus emulate the standby console on the active supervisor engine. Only one active standby console session is active at any time.		
	The Virtual Console for Standby Supervisor Engine allows users who are logged onto the active supervisor engine to remotely execute show commands on the standby supervisor engine and view the results on the active supervisor engine. Virtual Console is available only from the active supervisor engine.		
	You can access the standby virtual console from the active supervisor engine with the attach module . session module , or remote login commands on the active supervisor engine. You must be in privilege EXEC mode (level 15) to run these commands to access the standby console.		
Note	The session module command is identical to the attach module <i>mod</i> and the remote login module <i>mod</i> commands.		

Once you enter the standby virtual console, the terminal prompt automatically changes to "<hostname>-standby-console#" where hostname is the configured name of the switch. The prompt is restored back to the original prompt when you exit the virtual console.

You exit the virtual console with the **exit** or **quit** commands. When the inactivity period of the terminal on the active supervisor engine where you logged in exceeds the configured idle time, you are automatically logged out of the terminal on the active supervisor engine. In such a case, the virtual console session is also terminated. Virtual console session is also automatically terminated when the standby is rebooted. After the standby boots up, you need to create another virtual console session.

The following limitations apply to the standby virtual console:

All commands on the virtual console run to completion. It does not provide the auto-more feature; it behaves as if the **terminal length 0** command has been executed. It is also non-interactive. Therefore, a running command cannot be interrupted or aborted by any key sequence on the active supervisor engine. Therefore if a command produces considerable output, the virtual console displays it on the supervisor screen.

The virtual console is non-interactive. Because the virtual console does not detect the interactive nature of a command, any command that requires user interaction causes the virtual console to wait until the RPC timer aborts the command.

The virtual console timer is set to 60 seconds. The virtual console returns to its prompt after 60 seconds. During this time, you cannot abort the command from the key board. You must wait for the timer to expire before you continue.

You cannot use virtual console to view debug and syslog messages that are being displayed on the standby supervisor engine. The virtual console only displays the output of commands that are executed from the virtual console. Other information that is displayed on the real standby console does not appear on the virtual console.

To login to the standby supervisor engine using a virtual console, do the following:

```
Switch# session module 2
Connecting to standby virtual console
Type "exit" or "quit" to end this session
```

Switch-standby-console# **exit** Switch#

If the standby console is not enabled, the following message appears.

Switch-standby-console# Standby console disabled. Valid commands are: exit, logout

Related Commands	Command	Description
	attach module	Remotely connects to a specific module.
	remote login module	Remotely connects to a specific module.

Examples

set

To mark IP traffic by setting a class of service (CoS), a Differentiated Services Code Point (DSCP), or IP-precedence in the packet, use the **set** policy-map class configuration command. To remove the traffic classification, use the **no** form of this command.

set {cos new-cos | [ip] {dscp new-dscp | precedence new-precedence} | qos group value}

no set cos *new-cos* | **ip** {**dscp** *new-dscp* | **precedence** *new-precedence*} | **qos group** *value*}

Syntax Description	cos new-cos	New CoS value assigned to the classified traffic. The range is 0 to 7.	
	ip dscp new-dscp	New DSCP value assigned to the classified traffic. The range is	
		0 to 63. You also can enter a mnemonic name for a commonly used	
		value. The specified value sets the type of service (ToS) traffic class	
		byte in the IPv4/IPv6 packet header.	
	ip precedence new-preced	<i>lence</i> New IP-precedence value assigned to the classified traffic. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value. The specified value sets the precedence bit in the IP header.	
	qos group value	Internal QoS group assigned to a classified packet on ingress to an interface.	
Defaults	No marking is enabled on p	packets.	
Command Modes	Policy-map class configuration	tion	
Command History	Release N	Modification	
	12.1(8a)EW S	Support for this command was introduced on the Catalyst 4500 series switch.	
	12.2(40)SG A	Added support for Supervisor Engine 6-E and Catalyst 4900M chassis.	
Usage Guidelines	You can use the set comma	nd only in class-level classes.	
	The set dscp <i>new-dscp</i> and the set precedence <i>new-precedence</i> commands are the same as the set ip dscp <i>new-dscp</i> and the set ip precedence <i>new-precedence</i> commands.		
	For the set dscp <i>new-dscp</i> or the set precedence <i>new-precedence</i> command, you can enter a mnemonic name for a commonly used value. For example, you can enter the set dscp af11 command, which is the as same entering the set dscp 10 command. You can enter the set precedence critical command, which is the same as entering the set precedence 5 command. For a list of supported mnemonics, enter the set dscp ? or the set precedence ? command to see the command-line help strings.		
	You can configure the set cos <i>new-cos</i> , set dscp <i>new-dscp</i> , or set precedence <i>new-precedence</i> command in an ingress and an egress policy map attached to an interface or VLAN.		

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Examples

This example shows how to create a policy map called p1 with CoS values assigned to different traffic types. Class maps for "voice" and "video-data" have already been created.

```
Switch# configure terminal
Switch(config)# policy-map p1
Switch(config-pmap)# class voice
Switch(config-pmap-c)# set cos 1
Switch(config-pmap)# exit
Switch(config-pmap)# class video-data
Switch(config-pmap-c)# set cos 2
Switch(config-pmap)# exit
Switch#
```

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

Related Commands	Command	Description
	class	Specifies the name of the class whose traffic policy you want to create or change.
	policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
	show policy-map	Displays information about the policy map.
	trust	Defines a trust state for traffic classified through the class policy-map configuration command.

set cos

To set the Layer 2 class of service (CoS) value of a packet, use the **set cos** command in policy-map class configuration mode. To remove a specific CoS value setting, use the **no** form of this command.

set cos {cos-value | from-field [table table-map-name]}

no set cos {*cos-value* | *from-field* [**table** *table-map-name*]}

Syntax Description	cos-value	Specific IEEE 802.1Q CoS value from 0 to 7.
	from-field	Specific packet-marking category to be used to set the CoS value of the packet. If you are using a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords are as follows:
		• precedence
		• dscp
		• cos
		• qos group
	table	(Optional) Indicates that the values set in a specified table map will be used to set the CoS value.
	table-map-name	(Optional) Name of the table map used to specify the CoS value. The table map name can be a maximum of 64 alphanumeric characters.
Command Default	No CoS value is set f	for the outgoing packet.
Command Modes	Policy-map class con	figuration
Command Modes	Policy-map class con	figuration
Command Modes	Policy-map class con Release 12.2(40)SG	figuration Modification Support for this command was introduced on the Catalyst 4500 series
Command Modes Command History	Policy-map class con Release 12.2(40)SG The set cos commandor or VLAN. You can use this com	Modification Support for this command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6-E and Catalyst 4900M chassis.
Command Modes Command History	Policy-map class con Release 12.2(40)SG The set cos commandor or VLAN. You can use this com	Modification Support for this command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6-E and Catalyst 4900M chassis. d can be used in an ingress as well as an egress policy map attached to an interface mand to specify the "from-field" packet-marking category to be used for mapping
Command Modes Command History	Policy-map class con Release 12.2(40)SG The set cos command or VLAN. You can use this com and setting the CoS w • Precedence	Modification Support for this command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6-E and Catalyst 4900M chassis. d can be used in an ingress as well as an egress policy map attached to an interface mand to specify the "from-field" packet-marking category to be used for mapping
Command Modes Command History	Policy-map class con Release 12.2(40)SG The set cos command or VLAN. You can use this com and setting the CoS w • Precedence	Modification Support for this command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6-E and Catalyst 4900M chassis. d can be used in an ingress as well as an egress policy map attached to an interface mand to specify the "from-field" packet-marking category to be used for mapping /alue. The "from-field" packet-marking categories are as follows: rvices code point (DSCP)

If you specify a "from-field" category but do not specify the **table** keyword and the applicable *table-map-name* argument, the default action will be to copy the value associated with the "from-field" category as the CoS value. For instance, if you configure the **set cos precedence** command, the precedence value will be copied and used as the CoS value.

You can do the same for the DSCP marking category. That is, you can configure the **set cos dscp** command, and the DSCP value will be copied and used as the CoS value.



If you configure the **set cos dscp** command, only the *first three bits* (the class selector bits) of the DSCP field are used.

<u>Note</u>

If you configure the **set cos qos group** command, only the three least significant bits of the qos group field are used.

Examples

This example shows how to configure a policy map called "cos-set" and assign different CoS values for different types of traffic. This example assumes that the class maps called "voice" and "video-data" have already been created.

```
Switch# configure terminal
Switch(config)# policy-map cos-set
Switch(config-pmap)# class voice
Switch(config-pmap-c)# set cos 1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video-data
Switch(config-pmap-c)# set cos 2
Switch(config-pmap-c)# end
Switch#
```

This example shows how to configure a policy map called "policy-cos" and to use the values defined in a table map called "table-map1". The table map called "table-map1" was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the **table-map** (value mapping) command page.

This example shows how the setting of the CoS value is based on the precedence value defined in "table-map1":

```
Switch# configure terminal
Switch(config)# policy-map policy-cos
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set cos precedence table table-map1
Switch(config-pmap-c)# end
Switch#
```

Related Commands	Command	Description
	match (class-map configuration)	Defines the match criteria for a class map.
	policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
	service-policy (policy-map class)	Creates a service policy that is a quality of service (QoS) policy within a policy map.

Command	Description	
set dscp	Marks a packet by setting the differentiated services code point (DSCP) value in the type of service (ToS) byte.	
set precedence	Sets the precedence value in the packet header.	
show policy-map	Displays information about the policy map.	
set dscp

To mark a packet by setting the differentiated services code point (DSCP) value in the type of service (ToS) byte, use the **set dscp** command in policy-map class configuration mode. To remove a previously set DSCP value, use the **no** form of this command.

set [ip] dscp {dscp-value | from-field [table table-map-name]}

no set [**ip**] **dscp** {*dscp-value* | *from-field* [**table** *table-map-name*]

Syntax Description	ір	(Optional) Specifies that the match is for IPv4 packets only. If not used, the match is on both IPv4 and IPv6 packets.	
	dscp-value	A number from 0 to 63 that sets the DSCP value. A mnemonic name for commonly used values can also be used.	
	from-field	Specific packet-marking category to be used to set the DSCP value of the packet. If you are using a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords are as follows:	
		• cos	
		• qos-group	
		• dscp	
		• precedence	
	table	(Optional) Used in conjunction with the <i>from-field</i> argument. Indicates that the values set in a specified table map will be used to set the DSCP value.	
	table-map-name	(Optional) Used in conjunction with the table keyword. Name of the table map used to specify the DSCP value. The name can be a maximum of 64 alphanumeric characters.	
Command Default	Disabled		
Command Modes	Policy-map class	configuration	
Command History	Release	Modification	
	12.2(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.	
	12.2(40)SG	Added support for 'from-field' for policy-map configured on a Supervisor Engine 6-E.	

Usage Guidelines Once the DSCP bit is set, other quality of service (QoS) features can then operate on the bit settings.

DSCP and Precedence Values Are Mutually Exclusive

The **set dscp** command cannot be used with the **set precedence** command to mark the *same* packet. The two values, DSCP and precedence, are mutually exclusive. A packet can have one value or the other, but not both.

You can use this command to specify the "from-field" packet-marking category to be used for mapping and setting the DSCP value. The "from-field" packet-marking categories are as follows:

- Class of service (CoS)
- QoS group
- Precedence
- Differentiated services code point (DSCP)

If you specify a "from-field" category but do not specify the **table** keyword and the applicable *table-map-name* argument, the default action will be to copy the value associated with the "from-field" category as the DSCP value. For instance, if you configure the **set dscp cos** command, the CoS value will be copied and used as the DSCP value.



The CoS field is a three-bit field, and the DSCP field is a six-bit field. If you configure the **set dscp cos** command, only the three bits of the CoS field will be used.

If you configure the **set dscp qos-group** command, the QoS group value will be copied and used as the DSCP value.

The valid value range for the DSCP is a number from 0 to 63. The valid value range for the QoS group is a number from 0 to 63.

Set DSCP Values in IPv6 Environments

When this command is used in IPv6 environments, the default match occurs on both IP and IPv6 packets. However, the actual packets set by this function are only those which meet the match criteria of the class-map containing this function.

Set DSCP Values for IPv6 Packets Only

To set DSCP values for IPv6 values only, the **match protocol ipv6** command must also be used. Without that command, the DSCP match defaults to match both IPv4 and IPv6 packets.

Set DSCP Values for IPv4 Packets Only

To set DSCP values for IPv4 packets only, use the **ip** keyword in the **match** command for classification. Without the **ip** keyword, the match occurs on both IPv4 and IPv6 packets.

Examples

Packet-marking Values and Table Map

In the following example, the policy map called "policy1" is created to use the packet-marking values defined in a table map called "table-map1". The table map was created earlier with the table-map (value mapping) command. For more information about the table-map (value mapping) command, see the table-map (value mapping) command page.

This example shows how the DSCP value is set according to the CoS value defined in the table map called "table-map1".

```
Switch# configure terminal
Switch(config)# policy-map policy1
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set dscp cos table table-map1
Switch(config-pmap-c) # end
Switch#
```

Command	Description	
match (class-map configuration)	Defines the match criteria for a class map.	
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.	
service-policy (policy-map class)	Creates a service policy that is a quality of service (QoS) policy within a policy map.	
set cos	Sets IP traffic by setting a class of service (CoS).	
set precedence	Sets the precedence value in the packet header.	
show policy-map	Displays information about the policy map.	
show policy-map interface	Displays the statistics and configurations of the input and output policies that are attached to an interface.	
table-map (value mapping) (refer to Cisco IOS documentation)	Modifies metric and tag values when the IP routing table is updated with BGP learned routes.	
	match (class-map configuration)policy-mapservice-policy (policy-map class)set cosset precedenceshow policy-mapshow policy-map interfacetable-map (value mapping) (refer to Cisco IOS	

Re

set precedence

To set the precedence value in the packet header, use the **set precedence** command in policy-map class configuration mode. To remove the precedence value, use the **no** form of this command.

set precedence {precedence-value | from-field [table table-map-name]}

no set precedence {*precedence-value* | *from-field* [**table** *table-map-name*]}

Syntax Description	precedence-value	A number from 0 to 7 that sets the precedence bit in the packet header.
	from-field	Specific packet-marking category to be used to set the precedence value of the packet. If you are using a table map for mapping and converting packet-marking values, this argument value establishes the "map from" packet-marking category. Packet-marking category keywords are as follows:
		• cos
		• qos-group
		• dscp
		• precedence
	table	(Optional) Indicates that the values set in a specified table map will be used to set the precedence value.
	table-map-name	(Optional) Name of the table map used to specify a precedence value based on the class of service (CoS) value. The name can be a maximum of 64 alphanumeric characters.
Command Default	Disabled	
Command Modes	Policy-map class cont	figuration
Command History	Release	Modification
	12.2(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(40)SG	Added support for 'from-field' for policy-map configured on a Supervisor Engine 6-E.
Usage Guidelines	Command Compatibility	,
,	The set precedence c	ommand cannot be used with the set dscp command to mark the <i>same</i> packet. The d precedence, are mutually exclusive. A packet can be one value or the other, but

You can use this command to specify the "from-field" packet-marking category to be used for mapping and setting the precedence value. The "from-field" packet-marking categories are as follows:

- CoS
- QoS group
- DSCP
- Precedence

If you specify a "from-field" category but do not specify the **table** keyword and the applicable *table-map-name* argument, the default action will be to copy the value associated with the "from-field" category as the precedence value. For instance, if you configure the **set precedence cos** command, the CoS value will be copied and used as the precedence value.

You can do the same for the QoS group-marking category. That is, you can configure the **set precedence qos-group** command, and the QoS group value will be copied and used as the precedence value.

The valid value range for the precedence value is a number from 0 to 7. The valid value range for the QoS group is a number from 0 to 63. Therefore, when configuring the **set precedence qos-group** command the three least significant bits of qos-group are copied to precedence.

Precedence Values in IPv6 Environments

When this command is used in IPv6 environments it can set the value in both IPv4 and IPv6 packets. However, the actual packets set by this function are only those that meet the match criteria of the class-map containing this function.

Setting Precedence Values for IPv6 Packets Only

To set the precedence values for IPv6 packets only, the **match protocol ipv6** command must also be used in the class-map that classified packets for this action. Without the **match protocol ipv6** command, the class-map may classify both IPv6 and IPv4 packets, (depending on other match criteria) and the **set precedence** command will act upon both types of packets.

Setting Precedence Values for IPv4 Packets Only

To set the precedence values for IPv4 packets only, use a command involving the **ip** keyword like the **match ip precedence** or **match ip dscp** command or include the **match protocol ip** command along with the others in the class map. Without the additional **ip** keyword, the class-map may match both IPv6 and IPv4 packets (depending on the other match criteria) and the **set precedence** or **set dscp** command may act upon both types of packets.

Examples

In the following example, the policy map named policy-cos is created to use the values defined in a table map named table-map1. The table map named table-map1 was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the **table-map** (value mapping) command page.

This example shows how the precedence value is set according to the CoS value defined in table-map1.

```
Switch# configure terminal
Switch(config)# policy-map policy-cos
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set precedence cos table table-map1
Switch(config-pmap-c)# end
Switch#
```

Related Commands	Command	Description
	match (class-map configuration)	Defines the match criteria for a class map.
	policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
	service-policy (policy-map class)	Creates a service policy that is a quality of service (QoS) policy within a policy map.
	set cos	Sets IP traffic by setting a class of service (CoS).
	set dscp	Marks a packet by setting the differentiated services code point (DSCP) value in the type of service (ToS) byte.
	set qos-group	Sets a quality of service (QoS) group identifier (ID) that can be used later to classify packets.
	set precedence	Sets the precedence value in the packet header.
	show policy-map	Displays information about the policy map.
	show policy-map interface	Displays the statistics and configurations of the input and output policies that are attached to an interface.
	table-map (value mapping) (refer to Cisco IOS documentation)	Modifies metric and tag values when the IP routing table is updated with BGP learned routes.

set qos-group

To set a quality of service (QoS) group identifier (ID) that can be used later to classify packets, use the **set qos-group** command in policy-map class configuration mode. To remove the group ID, use the **no** form of this command.

set qos-group group-id

no set qos-group group-id

Syntax Description	group-id	Group ID number in the range from 0 to 63.
Command Default	The group ID is se	t to 0.
Command Modes	Policy-map class c	onfiguration
Command History	Release	Modification
	12.2(40)SG	Support for this command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6-E and Catalyst 4900M chassis
Usage Guidelines	through a service-	command allows you to associate a group ID with a packet. This association is made policy attached to an interface or VLAN in the input direction. The group ID can be utput direction to apply QoS service policies to the packet.
Examples	This example show	vs how to set the qos-group to 5:
	This example shows how to set the qos-group to 5: Switch#configure terminal Switch(config)#policy-map p1 Switch(config-pmap)#class c1 Switch(config-pmap-c)#set qos Switch(config-pmap-c)#set qos-group 5 Switch(config-pmap-c)#end Switch#	

Related Commands	Command	Description
	match (class-map configuration)	Defines the match criteria for a class map.
	policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
	service-policy (policy-map class)	Creates a service policy that is a quality of service (QoS) policy within a policy map.
	show policy-map	Displays information about the policy map.
	show policy-map interface	Displays the statistics and configurations of the input and output policies that are attached to an interface.

shape (class-based queueing)

To enable traffic shaping a class of traffic in a policy map attached to a physical port, use the **shape average** policy-map class command. Traffic shaping limits the data transmission rate. To return to the default setting, use the **no** form of this command.

shape average {rate} [bps | kbps | mbps | gbps]

shape average percent {percent_value}

no shape average

(Optional) Specifies a rate in gigabits per seconds.		
Specifies a percentage of bandwidth for traffic shaping.		
<i>percent_value</i> (Optional) Specifies a percentage of the bandwidth used for traffic shaping; valid values are from 1 to 100 percent.		
yst 4500 series switch using a		
l: 		

Shaping is the process of delaying out-of-profile packets in queues so that they conform to a specified profile. Shaping is distinct from policing. Policing drops packets that exceed a configured threshold, but shaping buffers packets so that traffic remains within the threshold. Shaping offers greater smoothness in handling traffic than policing.

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

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

 Examples
 This example shows how to limit the specified traffic class to a data transmission rate of 256 kbps:

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

 Switch(config)# policy-map policy1
 Switch(config-pmap)# class class1

 Switch(config-pmap-c)# shape average 256000
 Switch(config-pmap-c)# exit

 Switch(config-pmap)# exit
 Switch(config-pmap)# exit

 Switch(config-if)# interface gigabitethernet1/1
 Switch(config-if)# service-policy output policy1

 Switch(config-if)# end
 Switch(config-if)# end

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

Related Commands	Command	Description
	bandwidth	Creates a signaling class structure that can be referred to by its name.
	class	Specifies the name of the class whose traffic policy you want to create or change.
	dbl	Enables active queue management on a transmit queue used by a class of traffic.
	policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
	service-policy (policy-map class)	Creates a service policy that is a quality of service (QoS) policy within a policy map.
	show policy-map	Displays information about the policy map.

shape (interface configuration)

To specify traffic shaping on an interface, use the **shape** command. To remove traffic shaping, use the **no** form of this command

shape [rate] [percent]

no shape [rate] [percent]

Syntax Description	rate	(Optional) Specifies an average rate for traffic shaping; the range is 16000 to 1000000000. Post-fix 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 tra	iffic 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.	
When the high shape rates are configured on the Ca (WS-X4013+10GE), the Catalyst 4500 Supervisor Supervisor Engine V-10GE (WS-X4516-10GE), the that involve contention and unusual packet size dist a Stub ASIC and connected to the backplane gigape achieved under worst-case conditions. On ports tha		is available on all the ports, and it sets an upper limit on the bandwidth. shape rates are configured on the Catalyst 4500 Supervisor Engine II-Plus-10GE GE), the Catalyst 4500 Supervisor Engine V (WS-X4516), and the Catalyst 4500 ne V-10GE (WS-X4516-10GE), the shaped traffic rate may not be achieved in situations tention and unusual packet size distributions. On the ports that are multiplexed through d connected to the backplane gigaports, the shape rates above 7 Mbps may not be worst-case conditions. On ports that are connected directly to the backplane gigaports, r engine gigaports, the shape rates above 50 Mbps may not be achieved under worst-case	
	-	of ports that are connected directly to the backplane are as follows:	
	 Uplink ports on Supervisor Engine II+, II+10GE, III, IV, V, and V-10GE Ports on the WS-X4306-GB module 		
	 The two 1000BASE-X ports on the WS-X4232-GB-RJ module 		
		o ports on the WS-X4418-GB module	
	• The two 100	00BASE-X ports on the WS-X4412-2GB-TX module	

Examples

All ports on the 24-port modules and the 48-port modules are multiplexed through a Stub ASIC. Some examples of ports multiplexed through a Stub ASIC are as follows:

- 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

This 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 access-group mode interface** command.

show access-group mode interface [interface interface-number]

Syntax Description	interface	<i>e</i> (Optional) Interface type; valid values are ethernet , fastethernet , gigabitethernet , tengigabitethernet , and port-channel .		
	interface-number	(Optional) Interface number.		
Defaults	This command has	no default settings.		
command Modes	Privileged EXEC mode			
Command History	Release	Modification		
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.		
	12.2(25)EW	Support for the 10-Gigabit Ethernet interface was introduced on the Catalyst 4500 series switch.		
Jsage Guidelines	The valid values for	the port number depend on the chassis used.		
xamples	This example shows how to display the ACL configuration on the Fast Ethernet interface			
	Switch# show acce Interface FastEth Access group m Switch#			
Related Commands	Command	Description		
	access-group mod	e Specifies the override modes (for example, VACL overrides PACL) and the non-override modes (for example, merge or strict mode).		

show adjacency

To display information about the Layer 3 switching adjacency table, use the show adjacency command.

Syntax Description	interface	(Optional) Interface type; possible valid values are ethernet , fastethernet , gigabitethernet , tengigabitethernet , pos , ge-wan , and atm .
	interface-number	(Optional) Module and port number; see the "Usage Guidelines" section for valid values.
	null interface-number	(Optional) Specifies the null interface; the valid value is 0 .
	port-channel number	(Optional) Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 256.
	vlan vlan-id	(Optional) Specifies the VLAN; valid values are from 1 to 4094.
	detail	(Optional) Displays the information about the protocol detail and timer.
	internal	(Optional) Displays the information about the internal data structure.
	summary	(Optional) Displays a summary of CEF-adjacency information.
Defaults	This command has	no default settings.
Command Modes	EXEC	
Command Modes	EXEC	
		Aodification
Command Modes	Release N	Aodification Extended to include the 10-Gigabit Ethernet interface.
Command History	ReleaseN12.2(25)EWE	Extended to include the 10-Gigabit Ethernet interface.
	ReleaseN12.2(25)EWEThe interface-number of example, if you specified	Extended to include the 10-Gigabit Ethernet interface. <i>ber</i> argument designates the module and port number. Valid values for lepend on the specified interface type and the chassis and module that are used. For ecify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module 13-slot chassis, valid values for the module number are from 1 to 13, and valid values
Command History	ReleaseN12.2(25)EWEThe interface-number of example, if you spect that is installed in a for the port number	Extended to include the 10-Gigabit Ethernet interface. <i>ber</i> argument designates the module and port number. Valid values for lepend on the specified interface type and the chassis and module that are used. For ecify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module 13-slot chassis, valid values for the module number are from 1 to 13, and valid values
Command History	ReleaseN12.2(25)EWEThe interface-number of example, if you spect that is installed in a for the port number Hardware Layer 3	Extended to include the 10-Gigabit Ethernet interface. <i>ber</i> argument designates the module and port number. Valid values for lepend on the specified interface type and the chassis and module that are used. For ecify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module 13-slot chassis, valid values for the module number are from 1 to 13, and valid values r are from 1 to 48. switching adjacency statistics are updated every 60 seconds.
Command History	ReleaseN12.2(25)EWEThe interface-number of example, if you spect that is installed in a for the port numbe Hardware Layer 3 The following info	Extended to include the 10-Gigabit Ethernet interface. <i>ber</i> argument designates the module and port number. Valid values for lepend on the specified interface type and the chassis and module that are used. For ecify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module a 13-slot chassis, valid values for the module number are from 1 to 13, and valid value r are from 1 to 48. switching adjacency statistics are updated every 60 seconds. prmation is contained in the show adjacency command:
Command History	ReleaseN12.2(25)EWEThe interface-number of example, if you spect that is installed in a for the port number Hardware Layer 3The following info• Protocol interf	Extended to include the 10-Gigabit Ethernet interface. <i>ber</i> argument designates the module and port number. Valid values for lepend on the specified interface type and the chassis and module that are used. For ecify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module 13-slot chassis, valid values for the module number are from 1 to 13, and valid values r are from 1 to 48. switching adjacency statistics are updated every 60 seconds. rmation is contained in the show adjacency command: Face.
Command History	ReleaseN12.2(25)EWEThe interface-number of example, if you spect that is installed in a for the port number Hardware Layer 3The following info• Protocol interface • Type of routing	Extended to include the 10-Gigabit Ethernet interface. <i>ber</i> argument designates the module and port number. Valid values for lepend on the specified interface type and the chassis and module that are used. For ecify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module 13-slot chassis, valid values for the module number are from 1 to 13, and valid value r are from 1 to 48. switching adjacency statistics are updated every 60 seconds. rrmation is contained in the show adjacency command: face. g protocol that is configured on the interface.
Command History	ReleaseN12.2(25)EWEThe interface-number of example, if you spect that is installed in a for the port numbeHardware Layer 3The following infoProtocol interfType of routingInterface addre	Extended to include the 10-Gigabit Ethernet interface. <i>ber</i> argument designates the module and port number. Valid values for lepend on the specified interface type and the chassis and module that are used. For ecify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module 13-slot chassis, valid values for the module number are from 1 to 13, and valid value r are from 1 to 48. switching adjacency statistics are updated every 60 seconds. rrmation is contained in the show adjacency command: face. g protocol that is configured on the interface.

- MAC address of the adjacent router.
- Time left before the adjacency rolls out of the adjacency table. After it rolls out, a packet must use the same next hop to the destination.

Examples

This example shows how to display adjacency information:

Switch# show adjacency				
Protocol	Interface	Address		
IP	FastEthernet2/3	172.20.52.1(3045)		
IP	FastEthernet2/3	172.20.52.22(11)		
Switch#				

This example shows how to display a summary of adjacency information:

```
Switch# show adjacency summary
Adjacency Table has 2 adjacencies
Interface Adjacency Count
FastEthernet2/3 2
Switch#
```

This example shows how to display protocol detail and timer information:

Switch# show adjacency detail				
Protocol	Interface	Address		
IP	FastEthernet2/3	172.20.52.2	1(3045)	
		0 packets,	0 bytes	
		000000000F1	F920000380000000000000	
		000000000000000	000000000000000000000000000000000000000	
		00605C865B2	2800D0BB0F980B0800	
		ARP	03:58:12	
IP	FastEthernet2/3	172.20.52.2	22(11)	
		0 packets,	0 bytes	
		000000000F1	F920000380000000000000	
		000000000000000	000000000000000000000000000000000000000	
		00801C93804	4000D0BB0F980B0800	
		ARP	03:58:06	
a '				

Switch#

This example shows how to display adjacency information for a specific interface:

Switch# :	show adjacency fastetherne	t2/3
Protocol	Interface	Address
IP	FastEthernet2/3	172.20.52.1(3045)
IP	FastEthernet2/3	172.20.52.22(11)
Switch#		

Related Commands	Command	Description	
	debug adjacency	Displays information about the adjacency debugging.	

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	Command	Description
	access-group mode	Specifies the override modes (for example, VACL overrides PACL) and the non-override modes (for example, merge or strict mode).
	arp access-list	Defines an ARP access list or adds clauses at the end of a predefined list.
	ip arp inspection filter vlan	Permits ARPs from hosts that are configured for static IP when DAI is enabled, defines an ARP access list, and applies the access list to a VLAN.

show auto install status

To display the status of an automatic installation, use the **show auto install status** command.

show auto install status

Syntax Description This	command has no argume	nts or keywords.
-------------------------	-----------------------	------------------

Command Modes Privileged EXEC mode

Command History	Release	Modification	
	12.2(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.	

Examples This example shows how to display the IP address of the TFTP server and to display whether or not the switch is currently acquiring the configuration file on the TFTP server:

Switch# show auto install status

```
Status: Downloading config fileDHCP Server: 20.0.0.1TFTP Server: 30.0.0.3Config File Fetched: Undetermined
```

The first IP address in the display indicates the server that is used for the automatic installation. The second IP address indicates the TFTP server that provided the configuration file.

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	interface interface-id	(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.		
	expression	(Optional) Expression in the output to use as a reference point.		
Command Modes	Privileged EXEC mode			
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 <i>interface-id</i> 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 on a			
	non-Supervisor Engine 6-E, 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 GigabitEthernet1/2 auto qos voip cisco-p Switch#	hone		
Related Commands	Command	Description		
	auto qos voip	Automatically configures quality of service (auto-QoS) for Voice over IP (VoIP) within a QoS domain.		

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	Switch> show F I Device Numb	
	File System MONLIB Offs Bad Sector Squeeze Log Squeeze Buf Num Spare S Spares: STATUS INFO: Writable NO File Ope Complete St NO Unrecove	<pre>= 1000000 Sector Size = 40000 Algorithm = 39 Erased State = FFFFFFF 0 Offset = 40000 Length = F40000 et = 100 Length = C628 Map Offset = 3FFF8 Length = 8 0 Offset = F80000 Length = 40000 fer Offset = FC0000 Length = 40000 ectors = 0</pre>

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
             D86EE0AD 957CE8 9 7470636 Sep 20 1999 13:48:49 rp.halley
2 .. image
6456088 bytes available (9534696 bytes used)
----- FILE SYSTEM STATUS------
 Device Number = 0
DEVICE INFO BLOCK: bootflash
 Magic Number
                     = 6887635 File System Vers = 10000
                                                          (1.0)
 Length
                     = 1000000 Sector Size = 40000
                                                 = FFFFFFFF
 Programming Algorithm = 39
                                Erased State
 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
                     = 0
 Num Spare Sectors
   Spares:
STATUS INFO:
 Writable
 NO File Open for Write
 Complete Stats
 No Unrecovered Errors
 No Squeeze in progress
USAGE INFO:
              = 917CE8 Bytes Available = 628318
 Bytes Used
 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 mode

 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 cable-diagnostics tdr

To display the test results for the TDR cable diagnostics, use the show cable-diagnostics tdr command.

show cable-diagnostics tdr {interface {interface interface-number}}

Note	This command will command.	be depreca	ated in future C	isco IOS releases.	Please use the diagnostic start
Syntax Description	interface interface	? Interface	type; valid valu	ies are fastethern	et and gigabitethernet.
	interface-number	Module a	and port number		
Defaults	This command has	no default	settings.		
Command Modes	Privileged EXEC n	node			
Command History	Release	Modifica	ation		
	12.2(25)SG	Support	for this comma	nd was introduce	d on the Catalyst 4500 series switch.
Usage Guidelines	The TDR test is supported on Catalyst 4500 series switches running Cisco IOS Release 12.2(25)SG for the following line cards only:				
	• WS-X4548-GB-RJ45				
	• WS-X4548-GB-RJ45V				
	• WS-X4524-GB-RJ45V				
	• WS-X4013+TS				
	• WS-C4948				
	• WS-C4948-10GE				
	The distance to the	fault is dis	played in meter	rs (m).	
Examples	This example show	's how to di	splay informati	on about the TDR	test:
	Switch# show cabl Interface Speed Gi4/13 0Mbps				Status Fault

Switch#

Table 2-13 describes the fields in the show cable-diagnostics tdr command output.

Field	Description	
Interface	Interface tested.	
Speed	Current line speed.	
Pair	Local pair name.	
Cable Length	Distance to the fault in meters (m).	
Channel	Pair designation (A, B, C, or D).	
Status	Pair status displayed is one of the following:	
	• Terminated—The link is up.	
	• Fault—Cable fault (open or short)	

Table 2-13 show cable-diagnostics tdr Command Output Fields

Related Commands

Command	Description
test cable-diagnostics tdr	Tests the condition of copper cables on 48-port 10/100/1000 BASE-T modules.

show cdp neighbors

To display detailed information about the neighboring devices that are discovered through CDP, use the **show cdp neighbors** command.

show cdp neighbors [type number] [detail]

Syntax Description	type	(Optional) Interface type that is connected to the neighbors about want information; possible valid values are ethernet , fastetherne gigabitethernet , tengigabitethernet , port-channel , and vlan .	
	number	(Optional) Interface number that is connected to the neighbors abo you want information.	out which
	detail	(Optional) Displays detailed information about a neighbor (or neighbor including network address, enabled protocols, hold time, and softworsion.	-
Defaults	This command h	nas no default settings.	
Command Modes	Privileged EXE	C mode	
Command History	Release	Modification	
-	12.2(25)EW	Extended to include the 10-Gigabit Ethernet interface.	
Jsage Guidelines		rd is supported in Catalyst 4500 series switches that are configured w	with a Supervise
Jsage Guidelines	Engine 2.	rd is supported in Catalyst 4500 series switches that are configured v el values are from 0 to 282; values from 257 to 282 are supported on	-
Jsage Guidelines xamples	Engine 2. The port-chann FWSM only.		_
	Engine 2. The port-chann FWSM only.	el values are from 0 to 282; values from 257 to 282 are supported on ows how to display the information about the CDP neighbors:	_
-	Engine 2. The port-chann FWSM only. This example sh Switch# show c	el values are from 0 to 282; values from 257 to 282 are supported on ows how to display the information about the CDP neighbors:	-
	Engine 2. The port-chann FWSM only. This example sh Switch# show c Capability Cod	 el values are from 0 to 282; values from 257 to 282 are supported on ows how to display the information about the CDP neighbors: dp neighbors es: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone 	n the CSM and
	Engine 2. The port-chann FWSM only. This example sh Switch# show c Capability Cod Device ID	 el values are from 0 to 282; values from 257 to 282 are supported on ows how to display the information about the CDP neighbors: dp neighbors es: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone Local Intrfce Holdtme Capability Platform Port I 	n the CSM and
-	Engine 2. The port-chann FWSM only. This example sh Switch# show c Capability Cod Device ID lab-7206	<pre>el values are from 0 to 282; values from 257 to 282 are supported on ows how to display the information about the CDP neighbors: dp neighbors es: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone Local Intrfce Holdtme Capability Platform Port I Eth 0 157 R 7206VXR Fas 0/</pre>	n the CSM and
-	Engine 2. The port-chann FWSM only. This example sh Switch# show c Capability Cod Device ID lab-7206 lab-as5300-1	el values are from 0 to 282; values from 257 to 282 are supported on ows how to display the information about the CDP neighbors: dp neighbors es: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone Local Intrfce Holdtme Capability Platform Port I Eth 0 157 R 7206VXR Fas 0/ Eth 0 163 R AS5300 Fas 0	n the CSM and
	Engine 2. The port-chann FWSM only. This example sh Switch# show c Capability Cod Device ID lab-7206 lab-as5300-1 lab-as5300-2	el values are from 0 to 282; values from 257 to 282 are supported on ows how to display the information about the CDP neighbors: dp neighbors es: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone Local Intrfce Holdtme Capability Platform Port I Eth 0 157 R 7206VXR Fas 0/ Eth 0 163 R AS5300 Fas 0 Eth 0 159 R AS5300 Eth 0	n the CSM and
	Engine 2. The port-chann FWSM only. This example sh Switch# show c Capability Cod Device ID lab-7206 lab-as5300-1 lab-as5300-2 lab-as5300-3	el values are from 0 to 282; values from 257 to 282 are supported on ows how to display the information about the CDP neighbors: dp neighbors es: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone Local Intrfce Holdtme Capability Platform Port I Eth 0 157 R 7206VXR Fas 0/ Eth 0 163 R AS5300 Fas 0 Eth 0 159 R AS5300 Eth 0 Eth 0 122 R AS5300 Eth 0	n the CSM and
	Engine 2. The port-chann FWSM only. This example sh Switch# show c Capability Cod Device ID lab-7206 lab-as5300-1 lab-as5300-2 lab-as5300-3 lab-as5300-4	el values are from 0 to 282; values from 257 to 282 are supported on ows how to display the information about the CDP neighbors: dp neighbors es: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone Local Intrfce Holdtme Capability Platform Port I Eth 0 157 R 7206VXR Fas 0/ Eth 0 163 R AS5300 Fas 0 Eth 0 159 R AS5300 Eth 0 Eth 0 122 R AS5300 Eth 0 Eth 0 132 R AS5300 Fas 0/	n the CSM and
	Engine 2. The port-chann FWSM only. This example sh Switch# show c Capability Cod Device ID lab-7206 lab-as5300-1 lab-as5300-2 lab-as5300-3	el values are from 0 to 282; values from 257 to 282 are supported on ows how to display the information about the CDP neighbors: dp neighbors es: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone Local Intrfce Holdtme Capability Platform Port I Eth 0 157 R 7206VXR Fas 0/ Eth 0 163 R AS5300 Fas 0 Eth 0 159 R AS5300 Eth 0 Eth 0 122 R AS5300 Eth 0	n the CSM and

Table 2-14 describes the fields that are shown in the example.

Field	Definition
Device ID	Configured ID (name), MAC address, or serial number of the neighbor device.
Local Intrfce	(Local Interface) The protocol that is used by the connectivity media.
Holdtme	(Holdtime) Remaining amount of time, in seconds, that the current device holds the CDP advertisement from a transmitting router before discarding it.
Capability	Capability code that is discovered on the device. This device type is listed in the CDP Neighbors table. Possible values are as follows:
	R—Router
	T—Transparent bridge
	B—Source-routing bridge
	S—Switch
	H—Host
	I—IGMP device
	r—Repeater
	P—Phone
Platform	Product number of the device.
Port ID	Protocol and port number of the device.

Table 2-14show cdp neighbors Field Descriptions

This example shows how to display detailed information about your CDP neighbors:

```
Switch# show cdp neighbors detail
_____
Device ID: lab-7206
Entry address(es):
 IP address: 172.19.169.83
Platform: cisco 7206VXR, Capabilities: Router
Interface: Ethernet0, Port ID (outgoing port): FastEthernet0/0/0
Holdtime : 123 sec
Version :
Cisco Internetwork Operating System Software
IOS (tm) 5800 Software (C5800-P4-M), Version 12.1(2)
Copyright (c) 1986-2002 by Cisco Systems, Inc.
advertisement version: 2
Duplex: half
-------
Device ID: lab-as5300-1
Entry address(es):
 IP address: 172.19.169.87
Switch#
```

Table 2-15 describes the fields that are shown in the example.

Field	Definition
Device ID	Name of the neighbor device and either the MAC address or the serial number of this device.
Entry address(es)	List of network addresses of neighbor devices.
[network protocol] address	Network address of the neighbor device. The address can be in IP, IPX, AppleTalk, DECnet, or CLNS protocol conventions.
Platform	Product name and number of the neighbor device.
Capabilities	Device type of the neighbor. This device can be a router, a bridge, a transparent bridge, a source-routing bridge, a switch, a host, an IGMP device, or a repeater.
Interface	Protocol and port number of the port on the current device.
Holdtime	Remaining amount of time, in seconds, that the current device holds the CDP advertisement from a transmitting router before discarding it.
Version:	Software version running on the neighbor device.
advertisement version:	Version of CDP that is being used for CDP advertisements.
Duplex:	Duplex state of connection between the current device and the neighbor device.

Table 2-15show cdp neighbors detail Field Descriptions

Related Commands	Command	Description
	show cdp (refer to Cisco IOS documentation)	Displays global CDP information, including timer and hold-time information.
	show cdp entry (refer to Cisco IOS documentation)	Displays information about a specific neighboring device discovered using Cisco Discovery Protocol (CDP).
	show cdp interface (refer to Cisco IOS documentation)	Displays information about the interfaces on which Cisco Discovery Protocol (CDP) is enabled.
	show cdp traffic (refer to Cisco IOS documentation)	Displays traffic information from the CDP table.

show class-map

To display class map information, use the show class-map command.

show class-map class_name

Syntax Description	class_name	Name of the cla	ass map			
Defaults	This command	has no default se	ttings.			
Command Modes	Privileged EXE	C mode				
Command History	Release	Modification				
	12.1(8a)EW	Support for t	his com	mand was	introduced	on the Catalyst 4500 series switch.
	12.2(25)SG	Displays resu	lts fror	n the full f	ow option.	
Examples	Switch# show of Class Map mat Match any Class Map mat Match any Class Map mat Match ip pr Class Map mat Switch# This example sh Switch# show of	the any classed the any classes the any classes the all ipp5 (interpretence 5 the all agg-2 (interpretence 1) the angle of the angle of	efault imple d 1) id 3) Jay clas	(id 0) (id 2)		r all class maps: r a specific class map:
	Assume there as	re two active flo	ws as sh	own belov	on Fast Et	hernet interface 6/1:
	SrcIp	DstIp	IpPro	ot SrcL4Pc	rt DstL4Po	ort
		192.168.20.20 192.168.20.20		6789 6789	81 21	
	With following burst value.	configuration, ea	ach flov	w will be po	oliced to a 1	000000 bps with an allowed 9000-byte
Note						dress command, these two flows are destination address.

```
Switch# config terminal
Enter configuration commands, one per line. End with \ensuremath{\texttt{CNTL}}\xspace/\ensuremath{\texttt{Z}}\xspace.
Switch(config) # class-map c1
Switch(config-cmap)# match flow ip source-address ip destination-address ip protocol 14
source-port 14 destination-port
Switch(config-cmap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c) # police 1000000 9000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastEthernet 6/1
Switch(config-if)# service-policy input p1
Switch(config-if)# end
Switch# write memory
Switch# show policy-map interface
FastEthernet6/1
class-map c1
   match flow ip source-address ip destination-address ip protocol 14 source-port 14
destination-port
1
policy-map p1
    class c1
       police 1000000 bps 9000 byte conform-action transmit exceed-action drop
I.
interface FastEthernet 6/1
  service-policy input p1
Switch# show class-map c1
 Class Map match-all c1 (id 2)
   Match flow ip source-address ip destination-address ip protocol 14 source-port 14
```

Related Commands	Command	Description
	class-map	Creates a class map to be used for matching packets to the class whose name you specify and to be used enter class-map configuration mode.
	show policy-map	Displays information about the policy map.
	show policy-map interface	Displays the statistics and configurations of the input and output policies that are attached to an interface.

destination-port

Switch#

show diagnostic content

To display test information about the test ID, test attributes, and supported coverage test levels for each test and for all modules, use the **show diagnostic content** command.

show diagnostic content module {all | num}

Syntax Description	all	Displays all the modules on the chassis.
-,	num	Module number.
Defaults	This command h	nas no default settings.
Command Modes	EXEC	
Command History	Release	Modification
	12.2(20)EWA	Support for this command was introduced on the Catalyst 4500 series switch.
	Switch# show d module 1:	iagnostic content module all
Examples	<pre>modules of the c Switch# show d module 1: Diagnostics t B/* - Bas P/V/* - Per D/N/* - Dis</pre>	iagnostic content module all est suite attributes: ic ondemand test / NA port test / Per device test / NA ruptive test / Non-disruptive test / NA
	X/* - Not F/* - Fix E/* - Alw A/I - Mon m/* - Man	y applicable to standby unit / NA a health monitoring test / NA ed monitoring interval test / NA ays enabled monitoring test / NA itoring is active / Monitoring is inactive datory bootup test, can't be bypassed / NA oing test, always active / NA
	ID Test Nam	e Testing Interval (day hh:mm:ss.ms)
	1) supervis 2) packet-m	emory-ongoing> **N****I*0 not configured emory-bootup> **D****I** not configured

module 6: Diagnostics test suite attributes: B/* - Basic ondemand test / NA P/V/* - Per port test / Per device test / NA $\rm D/N/\star$ - Disruptive test / Non-disruptive test / NA $\ensuremath{\mathsf{S}}\xspace/*$ - Only applicable to standby unit / NA $\ensuremath{\mathbb{X}}\xspace/*$ – Not a health monitoring test / NA $\ensuremath{\mathsf{F}}\xspace/*$ – Fixed monitoring interval test / NA E/* - Always enabled monitoring test / NA A/I - Monitoring is active / Monitoring is inactive $\ensuremath{\texttt{m}}\xspace \star$ - Mandatory bootup test, can't be by passed / NA o/* - Ongoing test, always active / NA Testing Interval ID Test Name Attributes (day hh:mm:ss.ms) 1) linecard-online-diag -----> **D****I** not configured Switch#

Related Commands	Command	Description
	show diagnostic result module	Displays the module-based diagnostic test results.
	show diagnostic result module test 2	Displays the results of the bootup packet memory test.
	show diagnostic result module test 3	Displays the results from the ongoing packet memory test.

show diagnostic result module

To display the 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]

slot-num all test test-id test-id-range all detail	 (Optional) Specifies the slot on which diagnostics are displayed. (Optional) Displays the diagnostics for all slots. (Optional) Displays selected tests on the specified module. (Optional) Specifies a single test ID. (Optional) Specifies a range of test IDs. (Optional) Displays the diagnostics for all tests. (Optional) Displays the complete test results.
test test-id test-id-range all detail	(Optional) Displays selected tests on the specified module.(Optional) Specifies a single test ID.(Optional) Specifies a range of test IDs.(Optional) Displays the diagnostics for all tests.
test-id test-id-range all detail	(Optional) Specifies a single test ID. (Optional) Specifies a range of test IDs. (Optional) Displays the diagnostics for all tests.
test-id-range all detail	(Optional) Specifies a range of test IDs.(Optional) Displays the diagnostics for all tests.
all detail	(Optional) Displays the diagnostics for all tests.
detail	
	(Optional) Displays the complete test results.
A summary of th	a tast results for all modules in the chassis is displayed
A summary of th	e test results for all modules in the chassis is displayed.
Privileged EXEC	mode
Thinkeget EALC	
Release	Modification
12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.
This example sho	ows how to display the summary results for all modules in the chassis:
_	
Switten# SHOW UI	agnostic result module
Current bootup	diagnostic level: minimal
module 1:	
Overall diagr	postic result. PISS
	evel at card bootup: bypass
Test results:	(. = Pass, F = Fail, U = Untested)
1) supervis	sor-bootup> U
—	nemory-bootup> U
3) packet-m	nemory-ongoing> U
module 4:	
Overall diagn	nostic result: PASS
Diagnostic le	evel at card bootup: minimal
Test results:	(. = Pass, F = Fail, U = Untested)
1) 1	d-online-diag> .
	12.2(18)EW This example sho Switch# show di Current bootup module 1: Overall diagr Diagnostic le Test results: 1) supervis 2) packet-m 3) packet-m module 4: Overall diagr Diagnostic le

```
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 the 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: .

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
```

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

To display the results of the bootup packet memory test, use the **show diagnostic result module test** command. The output indicates whether the test passed, failed, or was not run.

show diagnostic result module $[N \mid all]$ [test *test-id*] [detail]

Syntax Description	N	Specifies the module number.
bymax bescription	all	Specifies all modules.
	test test-id	Specifies the number for the tdr test on the platform.
	detail	(Optional) Specifies the display of detailed information for analysis
		This option is recommended.
Defaults	Non-detailed result	5
Command Modes	EXEC mode	
Command History	Release	Modification
Usage Guidelines	12.2(25)SG	This command was introduced on the Catalyst 4500 series switch. is intended for use by Cisco support personnel when analyzing failures.
	12.2(25)SG The detail keyword This example shows	
Usage Guidelines Examples	12.2(25)SG The detail keyword This example shows	is intended for use by Cisco support personnel when analyzing failures. s how to display the results of the bootup packet memory tests:
-	12.2(25)SG The detail keyword This example shows Switch# show diag module 6:	is intended for use by Cisco support personnel when analyzing failures. s how to display the results of the bootup packet memory tests: nostic result module 6 detail
-	12.2(25)SG The detail keyword This example shows Switch# show diag module 6: Overall diagnos	is intended for use by Cisco support personnel when analyzing failures. s how to display the results of the bootup packet memory tests: nostic result module 6 detail
-	12.2(25)SG The detail keyword This example shows Switch# show diag module 6: Overall diagnos Test results:(.	is intended for use by Cisco support personnel when analyzing failures. s how to display the results of the bootup packet memory tests: nostic result module 6 detail tic result:PASS

Slot Ports Card Type Diag Status Diag Details ____ ____ 48 10/100/1000BaseT (RJ45)V, Cisco/IEEE Passed 6 None Detailed Status -----U = Unknown . = Pass L = Loopback failure S = Stub failure I = Ilc failure P = Port failure E = SEEPROM failure G = GBIC integrity check failure Ports 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 Ports 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 Ports 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 • 2) online-diag-tdr: Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 _____ Port 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 _____ Error code -----> 0 (DIAG_SUCCESS) Total run count -----> 1 Last test execution time -----> Jan 22 2001 03:01:54 First test failure time -----> n/a Last test failure time -----> n/a Last test pass time -----> Jan 22 2001 03:01:54 Total failure count -----> 0 Consecutive failure count -----> 0 Detailed Status _____ TDR test is in progress on interface Gi6/1

Switch#

Related Commands

Command diagnostic start
 Description

 Runs the specified diagnostic test.
2-435

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 analysi				
Defaults	Non-detailed results				
Command Modes	EXEC mode				
Command History	Release Modification				
	12.2(18)EWThis 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				

```
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 Command Description diagnostic monitor action Directs the action of the switch when it detects a packet memory failure.

show diagnostic result module Displays the results from the ongoing packet memory test.
test 3

show diagnostic result module test 3

To display the 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	N Module number.					
	detail	(Optional) Specifies the display of detailed information for analysis.				
Defaults	Non-detailed result	ts				
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 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 the 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-mer	mory-ongoing> .				
	Total 1 Last te First t Last te Last te	code> 0 (DIAG_SUCCESS) run count> 0 est execution time> n/a test failure time> n/a est failure time> n/a est pass time> n/a failure count> 0				
		utive failure count> 0 n free list: 64557 bad: 0 used for ongoing tests: 979				

```
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	Command	Description
	diagnostic monitor action	Directs the action of the switch when it detects a packet memory failure.
	show diagnostic result module test 2	Displays the results of the bootup packet memory test.

show dot1x

To display the 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 interface-i	<i>id</i> (Optional) Displays the 802.1X status for the specified port.		
Oyntax Description	statistics	(Optional) Displays the 802.1X statistics for the specified pole.		
	all	(Optional) Displays per-interface 802.1X configuration information for all interfaces with a non-default 802.1X configuration.		
Defaults	This command has no	o default settings.		
Command Modes	Privileged EXEC mo	de		
Command History	Release N	Adification		
	12.1(12c)EW S	support for this command was introduced on the Catalyst 4500 series switch.		
	12.1(19)EW D	Display enhanced to show the guest-VLAN value.		
		Support for the 10-Gigabit Ethernet interface was introduced on the Catalyst 450 series switch.		
		Support for currently-assigned reauthentication timer (if the timer is configured to onor the Session-Timeout value) was added.		
	12.2(31)SG S	support for port direction control and critical recovery was added.		
Usage Guidelines	• • • •	an interface, the global parameters and a summary are displayed. If you specify an		
	interface, the details for that interface are displayed.			
	If you enter the statistics keyword without the interface option, the statistics are displayed for all interfaces. If you enter the statistics keyword with the interface option, the statistics are displayed for the specified interface.			
	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.			
		nmand displays the currently assigned reauthentication timer and time remaining on, if reauthentication is enabled.		

Examples

This example shows how to display the output from the show dot1x command:

```
Switch# show dot1x
Sysauthcontrol = Disabled
Dot1x Protocol Version = 2
Dot1x Oper Controlled Directions = Both
Dot1x Admin Controlled Directions = Both
Critical Recovery Delay = 500
Critical EAP = Enabled
Switch#
```

This example shows how to display the 802.1X statistics for a specific port:

```
Switch# show dot1x interface fastethernet6/1
Dot1x Info for FastEthernet6/1
_____
                      = AUTHENTICATOR
PAE
PortControl
                     = AUTO
ControlDirection
                     = Both
                     = MULTI_DOMAIN
HostMode
ReAuthentication
                     = Disabled
QuietPeriod
                     = 60
                      = 30
ServerTimeout
SuppTimeout
                      = 30
                      = 3600 (Locally configured)
ReAuthPeriod
ReAuthMax
                      = 2
                      = 2
MaxReq
TxPeriod
                      = 30
RateLimitPeriod
                       = 0
Dot1x Authenticator Client List
Domain
                      = DATA
      ant = 0000.0000.ab01
Auth SM State = AUTHENTICATED
Supplicant
      Auth BEND SM Stat = IDLE
Port Status
                      = AUTHORIZED
Authentication Method = Dot1x
Authorized By
                      = Authentication Server
Vlan Policy
                      = 12
Domain
                      = VOICE
Supplicant
                      = 0060.b057.4687
      Auth SM State = AUTHENTICATED
      Auth BEND SM Stat = IDLE
            = AUTHORIZED
Port Status
Authentication Method = Dot1x
Authorized By
                     = Authentication Server
```

Switch#

Note

Table 2-16 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 802.1X specification.

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 con (allowed or disallowed).		

Table 2-16	show dot1x interface	Field Description

This is an example of output from the **show dot1x statistics interface gigabitethernet1/1** command. Table 2-17 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#
```

Table 2-17	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.
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

s Cor	mmand	Description		
dot	t1x critical	Enables the 802.1X critical authentication on a port.		
dot	t1x critical eapol	Enables sending EAPOL success packets when a port is critically authorized partway through an EAP exchange.		
dot	t1x critical recovery delay	Sets the time interval between port reinitializations.		
dot	t1x critical vlan	Assigns a critically authenticated port to a specific VLAN.		
dot	t1x guest-vlan	Enables a guest VLAN on a per-port basis.		
dot	t1x max-reauth-req	Sets the maximum number of times that the switch will retransmit an EAP-Request/Identity frame to the client before restarting the authentication process.		
dot	t1x port-control	Enables manual control of the authorization state on a port.		
ma	c-address-table notification	Enables MAC address notification on a switch.		

_ _

_ _

Sensor Status

PS1 PWR-C45-1400AC AC 1400W good good n.a.

_ _

Supply Model No Type Status

show environment

To display the environment alarm, operational status, and current reading for the chassis, use the **show** environment command.

show environment [alarm] | [status [chassis | fantray | powersupply | supervisor]] | [temperature]

alarm	(Ontional) Spec	rifies the alarm status of the	chassis		
fantray	(Optional) Specifies the status of the fan tray, and shows fan tray power consumption.				
powersupply	(Optional) Specifies the status of the power supply.				
supervisor	(Optional) Specifies the status of the supervisor engine.				
temperature	(Optional) Spec	cifies the current chassis ten	nperature readi	ngs.	
This command	nas no default sett	ings.			
Privileged EXE	C mode				
Release	Modification				
12.1(8a)EW	12.1(8a)EWSupport for this command was introduced on the Catalyst 4500 series switch.				
12.1(12c)EW	2.1(12c)EW Support for the ability to display generic environment information with the show environment command was added.				
	nows how to displ				
	ture readings for t		vironment aları	ns, operational status, and	
current tempera Switch# show e no temperature Module Sensor	ture readings for t nvironment alarms	he chassis: Temperature	Status	-	
current tempera Switch# show e no temperature Module Sensor	ture readings for t nvironment alarms	Temperature	Status	-	
current tempera Switch# show e no temperature Module Sensor	ture readings for t nvironment alarms	he chassis: Temperature	Status	-	
current tempera Switch# show e no temperature Module Sensor 	ture readings for t nvironment alarms	Temperature 22C (41C,56C,66C)	Status -+ ok	-	
current tempera Switch# show e no temperature Module Sensor 1 air in 1 air ou 1 air ou 3 air in	ture readings for t nvironment alarms let tlet (back) tlet (front) let	Temperature 22C (41C,56C,66C) 24C (45C,59C,69C) 22C (43C,57C,67C) 33C (51C,65C,68C)	Status -+ ok ok ok ok ok	-	
current tempera Switch# show e no temperature Module Sensor 1 air in 1 air ou 1 air ou 3 air ou 3 air ou	ture readings for t nvironment alarms let tlet (back) tlet (front) let tlet	Temperature 22C (41C,56C,66C) 24C (45C,59C,69C) 22C (43C,57C,67C) 33C (51C,65C,68C) 39C (69C,83C,86C)	Status ok ok ok ok ok ok ok	-	
current tempera Switch# show e no temperature Module Sensor 1 air in 1 air ou 1 air ou 3 air in	ture readings for t nvironment alarms let tlet (back) tlet (front) let tlet tlet	Temperature 22C (41C,56C,66C) 24C (45C,59C,69C) 22C (43C,57C,67C) 33C (51C,65C,68C)	Status -+ ok ok ok ok ok	-	
	supervisor temperature This command I Privileged EXE Release 12.1(8a)EW 12.1(12c)EW	status (Optional) Spector chassis (Optional) Spector fantray (Optional) Spector powersupply (Optional) Spector supervisor (Optional) Spector supervisor (Optional) Spector temperature (Optional) Spector This command has no default settor Privileged EXEC mode Release Modification 12.1(8a)EW Support for the environment of	status (Optional) Specifies the operational status chassis (Optional) Specifies the operational status fantray (Optional) Specifies the status of the fan tra powersupply (Optional) Specifies the status of the powersuper supervisor (Optional) Specifies the status of the super temperature (Optional) Specifies the status of the super temperature (Optional) Specifies the current chassis ten This command has no default settings. Privileged EXEC mode Release Modification 12.1(8a)EW Support for this command was introduced 12.1(12c)EW Support for the ability to display generic environment command was added.	status (Optional) Specifies the operational status information. chassis (Optional) Specifies the operational status of the chassis. fantray (Optional) Specifies the status of the fan tray, and shows fa powersupply (Optional) Specifies the status of the fan tray, and shows fa powersupply (Optional) Specifies the status of the power supply. supervisor (Optional) Specifies the status of the supervisor engine. temperature (Optional) Specifies the current chassis temperature readi This command has no default settings. Privileged EXEC mode Release Modification 12.1(8a)EW Support for this command was introduced on the Catalys 12.1(12c)EW Support for the ability to display generic environment inf environment command was added. Image: Status added.	

PS2 none

```
Power supplies needed by system : 1
Power supplies currently available : 1
Chassis Type : WS-C4507R-E
Power consumed by backplane : 40 Watts
Switch Bandwidth Utilization : 0%
Supervisor Led Color : Green
Module 1 Status Led Color : Green
Module 2 Status Led Color : Green
Module 3 Status Led Color : Green
Module 4 Status Led Color : Green
Fantray : Good
Power consumed by Fantray : 135 Watts
Switch#
```

This example shows how to display information about the environment alarms:

Switch# **show environment alarm** no alarm Switch#

This example shows how to display information about the power supplies, chassis type, and fan trays:

Switch# show environment status Power Fan Supply Model No Туре Status Sensor _____ _____ PWR-C45-1400AC AC 1400W good PS1 good PS2 -- -none _ _ Power Supply Max Min Max Min Absolute (Nos in Watts) Inline Inline System System Maximum Absolute _____ _____ 0 0 1360 1360 PS1 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-C4507R 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#
```

Catalyst 4500 Series Switch Cisco IOS Command Reference—Release 12.2(46)SG

This example shows how to display information about the power supply:

Switch#	show environment	status powe	ersupply	
Power				Fan
Supply	Model No	Туре	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 the 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 mode

Command HistoryReleaseModification12.1(8a)EWSupport for this command was introduced on the Catalyst 4500 series switch.12.1(19)EWDisplay includes the status of storm control.

Examples

This example shows how to display the error disable detection status:

Switch# show errdisa	able 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
12ptguard	Enabled
gbic-invalid	Enabled
dhcp-rate-limit	Enabled
unicast-flood	Enabled
storm-control	Enabled
ilpower	Enabled
arp-inspection Switch#	Enabled

Related Commands	Command	Description
	errdisable detect	Enables error-disable detection.
	errdisable recovery	Configures the recovery mechanism variables.
	show interfaces status	Displays the interface status or a list of interfaces in error-disabled state.

show errdisable recovery

To display error disable recovery timer information, use the show errdisable recovery command.

show errdisable recovery

Syntax Description	This command has	s no arguments o	or keywords.
--------------------	------------------	------------------	--------------

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

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 errdis ErrDisable Reason	-	
udld	Disabled	
bpduguard	Disabled	
security-violatio	Disabled	
channel-misconfig	Disabled	
vmps	Disabled	
pagp-flap	Disabled	
dtp-flap	Disabled	
link-flap	Disabled	
12ptguard	Disabled	
psecure-violation	Disabled	
gbic-invalid	Disabled	
dhcp-rate-limit	Disabled	
unicast-flood	Disabled	
storm-control	Disabled	
arp-inspection	Disabled	
Timer interval:30 s	econds	
Interfaces that will	l be enabled at	the next timeout:
Interface Errdisa	able reason	Time left(sec)
Fa7/32 arg	p-inspect	13

Related Commands	Command	Description
	errdisable detect	Enables error-disable detection.
	errdisable recovery	Configures the recovery mechanism variables.
	show interfaces status	Displays the interface status or a list of interfaces in error-disabled state.

show etherchannel

To display EtherChannel information for a channel, use the show etherchannel command.

Syntax Description	channel-group	(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 h	as no default settings.				
Command Modes Privileged EXEC mode						
Command History	Release	Modification				
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.				
	12.1(13)EWSupport for LACP was added to this command.					
Usage Guidelines	In the output belo means that the pl	ccify a channel group, all channel groups are displayed. ow, the Passive port list field is displayed for Layer 3 port channels only. This field hysical interface, which is still not up, is configured to be in the channel group (and he only port channel in the channel group).				
Examples	This example sho	ows how to display port-channel information for a specific group:				
	Switch# show etherchannel 1 port-channel Port-channels in the group:					
	Port-channel: F					
	FOIC-CHAIMEI, F	201				

```
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
_____
           = EC-Enbld Down Not-in-Bndl Usr-Config
Port state
Channel group = 1Mode = DesirableGcchange = 0Port-channel = nullGC = 0x00000000Psudo-agport
Port-channel = null
                                             Psudo-aqport = Po1
                      Load = 0x00
Port indx
           = 0
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.H - Hello timer is running.Q - Quit timer is running.
Timers: H - Hello timer is running.
      S - Switching timer is running. I - Interface timer is running.
Local information:
                             Hello Partner PAgP
                                                     Learning Group
        Flags State Timers Interval Count Priority Method Ifindex
Port
Fa5/4
        d U1/S1
                             1s
                                      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 = 1Mode = DesirableGcchange = 0Port-channel = nullGC = 0x00000000Psudo-agport
                                           Psudo-agport = Pol
Port indx = 0
                        Load = 0x00
Flags: S - Device is sending Slow hello. C - Device is in Consistent state.
S - Switching timer is running. I - Interface timer is running.
Local information:
                            Hello Partner PAgP
                                                     Learning Group
Port.
       Flags State Timers Interval Count Priority Method Ifindex
Fa5/5 d U1/S1
                            1s
                                    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
                               HotStandBy port = null
                 = 0 \times 000000000
GC
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:

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-Enbld Down Not-in-Bndl Usr-Config
Channel group = 1 Mode = Desirable Gcchange = 0
Port-channel = null GC = 0x00000000 Psudo-agport = Pol
Port indx = 0 Load = 0x00
Port indx
            = 0
                         Load = 0x00
Flags: S - Device is sending Slow hello. C - Device is in Consistent state.
       A - Device is in Auto mode.H - Hello timer is running.P - Device learns on physical port.Q - Quit timer is running.
Timers: H - Hello timer is running.
       S - Switching timer is running. I - Interface timer is running.
Local information:
                            Hello Partner PAgP Learning Group
        Flags State Timers Interval Count Priority Method Ifindex
Port
Fa5/4
        d U1/S1
                             1s
                                      0
                                              128
                                                        Any
                                                                 0
Age of the port in the current state: 02h:40m:35s
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 Psudo-agport = Pol
Port indx = 0 Load = 0x00
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.
<...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	Command	Description
	channel-group	Assigns and configures an EtherChannel interface to an EtherChannel group.
	interface port-channel	Accesses or creates a port-channel interface.

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 interface	(Optional) Displays the status on a specific interface.
Defaults	This command ha	s no default settings.
Command Modes	Privileged EXEC	mode
Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(25)EW	Support for the 10-Gigabit Ethernet interface was introduced on the Catalyst 4500 series switch.

Usage Guidelines Table 2-18 describes the fields in the **show flowcontrol** command output.

Table 2-18show 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.

Switch# show flowcontrol						
Port	Send Flo admin	wControl oper	Receive admin	FlowControl oper	RxPause	TxPause
Tel/1	off	off	on	off	0	0
Tel/2	off	off	on	off	0	0
Gi1/3	off	off	desired	on	0	0
Gi1/4	off	off	desired	on	0	0
Gi1/5	off	off	desired	on	0	0
Gi1/6	off	off	desired	on	0	0
Gi3/1	off	off	desired	off	0	0
Gi3/2	off	off	desired	off	0	0
Gi3/3	off	off	desired	off	0	0
Gi3/4	off	off	desired	off	0	0
Gi3/5	off	off	desired	off	0	0
Gi3/6	off	off	desired	off	0	0
Switch#						

This example shows how to display the flow control status on all the Gigabit Ethernet interfaces:

Examples

This example shows how to display the flow control status on module 1:

Switch#	show flow	wcontrol m	nodule 1			
Port	Send Flow	wControl	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 Gigabit Ethernet interface 3/4:

Switch#show flowcontrolinterfacegigabitethernet3/4PortSend FlowControlReceiveFlowControlRxPauseTxPauseadminoperadminoper---------------Gi3/4offoffonon00Switch#------------------------

This example shows how to display the flow control status on 10-Gigabit Ethernet interface 1/1:

Switch#	show flowco	ontrol int	erface t	engigabiteth	ernet1/1	
Port	Send Flo	owControl	Receive	FlowControl	RxPause	e TxPause
	admin	oper	admin	oper		
Te1/1 Switch#	off	off	on	off	0	0

Related Commands

s	Command	Description
	channel-group	Configures a Gigabit Ethernet interface to send or receive pause frames.
	show interfaces status	Displays the interface status or a list of interfaces in error-disabled state.

show hw-module port-group

To display how the X2 holes on a module are grouped, use the **show hw-module port-group** command.

show hw-module module number port-group

Syntax Description	module	Specifies	a line module.
	number	Specifies	a slot or module number.
	port-group	Specifies	a port-group on a switch.
Defaults	X2 mode.		
Command Modes	Global configu	ration mode	
Command History	Release	Modification	
	12.2(40)SG	Support for WS-X	X4606-10GE-E Twin Gigabit convertor introduced.
Usage Guidelines	dynamically. The TenGigabit and avoid having po- independent. The TenGigabit <slo In the Supervise engine through 10-Gigabit port Gigabit (TwinG</slo 	he terminology must r 1-Gigabit ports are n orts named TenGigabit he WS-X4606-10GE- it-num>/<1-6>, and th or Engine 6-E and Ca a stub ASIC. This stu s cannot be mixed on big Converter and SFF	d or disabled, the number and type of ports on the linecard change reflect this behavior. In Cisco IOS, 10-Gigabit ports are named amed Gigabit. Starting with Cisco IOS Release 12.2(40)SG, to t1/1 and Gigabit1/1, the 10-Gigabit and 1-Gigabit port numbers are E module with six X2 ports are named he SFP ports are named Gigabit <slot-num>/<7-18. talyst 4900M chassis, the ports are connected to the switching the ASIC imposes some limitations on the ports: Gigabit and a single stub ASIC; they must either be all 10-Gigabit (X2), or all P). The faceplates of X2 modules show this stub-port grouping, ng, or a box drawn around a grouping.</slot-num>
Examples	Switch# show h	w-module module 1 port-g	•
	Module Port 1 1 1 2 Switch#	-group Active Te1/1-3 Te1/4-6	Inactive Gi1/7-12 Gi1/13-18
Related Commands	Command		Description
	hw-module po	ort-group	Selects either Gigabit Ethernet or Ten Gigabit Ethernet interfaces on your module.

show hw-module uplink

To display the current uplink mode, use the show hw-module uplink command.

show hw-module uplink Defaults This command has no default settings. **Command Modes** Privileged EXEC mode **Command History** Release Modification 12.2(25)EW Support for this command was introduced on the Catalyst 4500 series switch. **Usage Guidelines** If the active uplink mode is different than configured mode, the output displays the change. By default, the current (operational) uplink selection is displayed. Examples This example shows the output displaying the current (active) uplinks: Switch# show hw-module uplink Active uplink configuration is TenGigabitEthernet This example shows the output for redundant systems in SSO mode if the 10-Gigabit Ethernet uplinks are active, and the Gigabit Ethernet uplinks are selected: Switch# show hw-module uplink Active uplink configuration is TenGigabitEthernet (will be GigabitEthernet after next reload) A 'redundancy reload shelf' or power-cycle of chassis is required to apply the new configuration This example shows the output for redundant systems in RPR mode if the 10-Gigabit Ethernet uplinks are active, and the Gigabit Ethernet uplinks are selected: Switch# show hw-module uplink Active uplink configuration is TenGigabitEthernet (will be GigabitEthernet after next reload) A reload of active supervisor is required to apply the new configuration. **Related Commands** Command Description hw-module uplink select Selects the 10-Gigabit Ethernet or Gigabit Ethernet uplinks on the Supervisor Engine V-10GE within the W-C4510R

chassis.

show idprom

To display the IDPROMs for the chassis, supervisor engine, module, power supplies, fan trays, clock module, and multiplexer (mux) buffer, use the **show idprom** command.

show idprom {all | chassis | module [mod] | interface int_name | supervisor | power-supply
 number | fan-tray}

C Description	all	Displays information for all IDPROMs.
	chassis	Displays information for the chassis IDPROMs.
	module	Displays information for the module IDPROMs.
	mod	(Optional) Specifies the module name.
	<pre>interface int_name</pre>	Displays information for the GBIC or SFP IDPROMs.
	supervisor	Displays information for the supervisor engine IDPROMs.
	power-supply number	Displays information for the power supply IDPROMs.
	fan-tray	Displays information for the fan tray IDPROMs.

Defaults

This command has no default settings.

Command Modes Privileged EXEC mode

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.
	12.2(25)EW	Support for the 10-Gigabit Ethernet interface was introduced on the Catalyst 4500 series switch.

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 = <tbd>
Hardware Revision = 0.2
Manufacturing Bits = 0x0000
 Engineering Bits = 0 \times 0000
 Snmp OID = 0.0.0.0.0.0.0.0
 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 = 0x000000000000000
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 idpror	n interface gigabitethernet1/2
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	= 130000000 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

Catalyst 4500 Series Switch Cisco IOS Command Reference—Release 12.2(46)SG

CC_BASE

= 0x1A

show idprom

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 = Unspecified BR, min Vendor Serial No. = K1273DH = 030409 Date code 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 SEEPROM contents (hex) size 128: 0x0000 01 00 01 00 00 00 00 00 00 00 00 01 0D 00 00 FFCISCO-FINISA 0x0010 00 00 00 00 43 49 53 43 4F 2D 46 49 4E 49 53 41 0x0020 52 20 20 20 00 00 90 65 46 54 52 2D 30 31 31 39 R ..^PeFTR-0119 -CSC B 0x0030 2D 43 53 43 20 20 20 20 42 20 20 20 00 00 1A 0x0040 00 1A 00 00 4B 31 32 37 33 44 48 20 20 20 20 20 20K1273DH 0x0050 20 20 20 20 30 33 30 34 30 39 20 20 64 00 00 B2 030409 d..2 29 00 02 80 22 33 38 3D C7 67 83 E8 DF 65 6A AF 0x0060)..^@"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 10-Gigabit Ethernet interface 1/1:

Switch# show idprom interface tengigabitethernet1/1

X2 Serial EEPROM Contents:	
Non-Volatile Register (NVR) Fields	
X2 MSA Version supported	:0xA
NVR Size in bytes	:0x100
Number of bytes used	:0xD0
Basic Field Address	:0xB
Customer Field Address	:0x77
Vendor Field Address	:0xA7
Extended Vendor Field Address	:0x100
Reserved	:0x0
Transceiver type	:0x2 =X2
Optical connector type	:0x1 =SC
Bit encoding	:0x1 =NRZ
Normal BitRate in multiple of 1M b/s	:0x2848
Protocol Type	:0x1 =10GgE
Standards Compliance Codes :	
10GbE Code Byte 0	:0x2 =10GBASE-LR
10GbE Code Byte 1	:0x0
SONET/SDH Code Byte 0	:0x0
SONET/SDH Code Byte 1	:0x0
SONET/SDH Code Byte 2	:0x0
SONET/SDH Code Byte 3	:0x0
10GFC Code Byte 0	:0x0
10GFC Code Byte 1	:0x0
10GFC Code Byte 2	:0x0
10GFC Code Byte 3	:0x0
Transmission range in 10m	:0x3E8
Fibre Type :	
Fibre Type Byte 0	:0x40 =NDSF only

Fibre Type Byte 1 :0x0 =Unspecified Centre Optical Wavelength in 0.01nm steps - Channel 0 :0x1 0xFF 0xB8 Centre Optical Wavelength in 0.01nm steps - Channel 1 :0x0 0x0 0x0 Centre Optical Wavelength in 0.01nm steps - Channel 2 :0x0 0x0 0x0 Centre Optical Wavelength in 0.01nm steps - Channel 3 :0x0 0x0 0x0 Package Identifier OUI :0xC09820 Transceiver Vendor OUI :0x3400800 Transceiver vendor name :CISCO-OPNEXT, INC Part number provided by transceiver vendor :TRT5021EN-SMC-W Revision level of part number provided by vendor :00 Vendor serial number :ONJ08290041 Vendor manufacturing date code :2004072000 Reserved1 : 00 02 02 20 D1 00 00 Basic Field Checksum :0x10 Customer Writable Area : 0x00: 58 32 2D 31 30 47 42 2D 4C 52 20 20 20 20 20 20 20 0x10: 20 20 20 20 20 4F 4E 4A 30 38 32 39 30 30 34 31 0x20: 31 30 2D 32 30 33 36 2D 30 31 20 20 41 30 31 20 Vendor Specific : 0x30: 00 00 00 00 11 E2 69 A9 2F 95 C6 EE D2 DA B3 FD 0x40: 9A 34 4A 24 CB 00 00 00 00 00 00 00 00 00 EF FC 0x50: F4 AC 1A D7 11 08 01 36 00 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 = 0 \times 0000
 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 = 0x000000000000000
 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-C4507R
 Serial Number = FOX04473737
 Part Number = 73 - 4289 - 02
Part Revision = 02
Manufacturing Deviation String = 0x00
Hardware Revision = 0.2
Manufacturing Bits = 0x0000
 Engineering Bits = 0 \times 0000
 Snmp OID = 0.0.0.0.0.0.0.0
Chassis Block Signature = 0x4001
Chassis Block Version = 1
Chassis Block Length = 22
Chassis Block Checksum = 421
Feature Bits = 0x000000000000000
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 - XXX - 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 = 0x0000000FFFFFFFF
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.
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} | {tengigabitethernet mod/interface-number} | {null interface-number} | vlan vlan_id} | status}]

Syntax Description	fastethernetmod/interface-numbergigabitethernetmod/interface-numbertengigabitethernetmod/interface-numbernull interface-number		(Optional) Specifies the Fast Ethernet module and interface.			
			(Optional) Specifies the Gigabit Ethernet module and interface. (Optional) Specifies the 10-Gigabit Ethernet module and interface.			
			(Optional) Specifies the null interface; the valid value is 0.			
	vlan vlan_id		(Optional) Specifies the VLAN; valid values are from 1 to 4094.			
	status		(Optional) Displays status information.			
Defaults Command Modes	This command h		ettings.			
Command Modes	Privileged EXEC	C mode	ettings.			
Command Modes	Privileged EXEO Release	C mode Modification				
Command Modes	Privileged EXEC Release 12.1(8a)EW	C mode Modification Support for t	his command was introduced on the Catalyst 4500 series switch.			
Defaults Command Modes Command History	Privileged EXEO Release	C mode Modification Support for t Support for e	his command was introduced on the Catalyst 4500 series switch. extended VLAN addresses was added. he 10-Gigabit Ethernet interface was introduced on the Catalyst 4500			

Usage Guidelines

s The statistics are collected on a per-VLAN basis for Layer 2 switched packets and Layer 3 switched packets. The statistics are available for both unicast and multicast. The Layer 3 switched packet counts are available for both the 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 that is displayed between the **show interfaces** command and the **show running-config** commands. The duplex mode that is displayed in the **show interfaces** command is the actual duplex mode that 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.

Linecards that support auto-MDIX configuration on their copper media ports include: WS-X4124-RJ45, WS-X4148-RJ with hardware revision 3.0 or higher, and WS-X4232-GB-RJ with hardware revision 3.0 or higher.

Examples

This example shows how to display traffic for Gigabit Ethernet interface 2/5:

Switch# show interfaces gigabitethernet2/5 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 traffic for 10-Gigabit Ethernet interface 1/1:

```
Switch# show interfaces tengigabitethernet1/1
Name: Tengigabitethernet1/1
Switchport: Enabled
Administrative Mode: private-vlan promiscuous trunk
Operational Mode: private-vlan promiscuous (suspended member of bundle Pol)
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: none
Trunking Native Mode VLAN: none
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: 202 (VLAN0202) 303 (VLAN0303) 304 (VLAN0304)
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk
Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: 802.1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Administrative private-vlan mapping trunk: New 202 (VLAN0202) 303 (VLAN0303) 304
(VLAN0304) 204 (VLAN0204) 305 (VLAN0305) 306 (VLAN0306)
```

```
Operational private-vlan: 202 (VLAN0202) 303 (VLAN0303) 304 (VLAN0304)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Switch#
```

This example shows how to verify the status of auto-MDIX on a RJ-45 port:

Note

You can verify the configuration setting and the operational state of auto-MDIX on the interface by entering the **show interfaces** EXEC command. This field is applicable and appears only on the **show interfaces** command output for 10/100/1000BaseT RJ45 copper ports on supported linecards including WS-X4124-RJ45, WS-X4148-RJ with hardware revision 3.0 or higher, and WS-X4232-GB-RJ with hardware revision 3.0 or higher.

```
FastEthernet6/3 is up, line protocol is up (connected)
  Hardware is Fast Ethernet Port, address is 0003.6ba8.ee68 (bia 0003.6ba8.ee68)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, link type is auto, media type is 10/100BaseTX
  input flow-control is unsupported output flow-control is unsupported
Auto-MDIX on (operational: on)
ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     157082 packets output, 13418032 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     1 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#	Switch# show interfaces gigabitethernet1/2 status					
Port	Name	Status	Vlan	Duplex	Speed Type	
Gi1/2		notconnect	1	auto	1000 1000-XWDM-RXONLY	
Switch#						

This example shows how to display status information for the interfaces on the supervisor engine:

Switch# show interfaces status

Port	Name	Status	Vlan	Duplex	Speed Type
Te1/1		connected	1	full	10G 10GBase-LR
Te1/2		connected	1	full	10G 10GBase-LR
Switch#					

L

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 mod	(Optional) Display information for the specified module only.
	interface	(Optional) Interface type; valid values are fastethernet , gigabitethernet , tengigabitethernet , and port-channel .
	interface-number	(Optional) Port number.
Defaults	This command has n	o default settings.
Command Modes	Privileged EXEC mc	ode
Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(25)EW	Support for the 10-Gigabit Ethernet interface was introduced on the Catalyst 4500 series switch.
	12.2(31)SGA	Support for auto-MDIX reflected in command output.
Usage Guidelines	<i>interface-number</i> dep 10/100-Mbps Fast Ef chassis, valid values Linecards that suppo	er argument designates the module and port number. Valid values for pend on the chassis and module used. For example, if you have a 48-port thernet RJ-21 (telco connector) switching module installed in a Catalyst 4507 for the slot number are from 2 to 13 and valid values for the port number are 1 to 48. rt auto-MDIX configuration on their copper media ports include: WS-X4124-RJ45, hardware revision 3.0 or higher, and WS-X4232-GB-RJ with hardware revision 3.0

Examples	This example shows how to display the interface capabilities for a module:				
		s 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 suppressio	n:percentage(0-100), hw			
	Flowcontrol:	<pre>rx-(off,on,desired),tx-(off,on,desired)</pre>			
	VLAN Membership:	static, dynamic			
	Fast Start:	yes			
	Queuing:	<pre>rx-(N/A), tx-(4q1t, Sharing/Shaping)</pre>			
	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			
		n: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				
	Link Debounce:	yes			
		no			
	Link Debounce Time:	no			
	Port Security	yes			
	Dot1x	yes			

This example shows how to display the interface capabilities for the 10-Gigabit Ethernet interface 1/1:

Switch# show interfaces tengigabitethernet1/1 capabilities

TenGigabitEthern	net1/1	
Model:		WS-X4517-X2
Type:		10GBase-LR
Speed:		10000
Duplex:		full
Trunk encap. t	ype:	802.1Q,ISL
Trunk mode:		on,off,desirable,nonegotiate
Channel:		yes
Broadcast supp	ression:	percentage(0-100), hw
Flowcontrol:		<pre>rx-(off,on),tx-(off,on)</pre>
VLAN Membershi	p:	static, dynamic
Fast Start:		yes

```
rx-(N/A), tx-(1p3q1t, Sharing/Shaping)
 Queuing:
 CoS rewrite:
                       yes
 ToS rewrite:
                       ves
 Inline power:
                      no
 SPAN:
                      source/destination
 UDLD:
                      yes
 Link Debounce:
                      no
 Link Debounce Time: no
 Port Security:
                  yes
 Dot1x:
                       yes
                      9198 bytes (Jumbo Frames)
 Maximum MTU:
 Multiple Media Types: no
 Diagnostic Monitoring: N/A
Switch#
```

This example shows how to display the interface capabilities for Gigabit Ethernet interface 1/1:

Switch# show interfaces gigabitethernet1/1 capabilities

SWICCHA SHOW INCELLACES	gigabitethermeti/i 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:	<pre>rx-(off,on,desired),tx-(off,on,desired)</pre>				
VLAN Membership:	static, dynamic				
Fast Start:	yes				
Queuing:	<pre>rx-(N/A), tx-(4q1t, Sharing/Shaping)</pre>				
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 the interface capabilities for Fast Ethernet interface 3/1:

Switch# show interfaces 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), $tx-(4qlt, Shaping)$
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#	

This example shows how to verify that the auto-MDIX configuration is supported on a port:

This example shows now to	verify that the auto-MDIA configuration is s
Switch# show interfaces :	fastethernet6/3 capabilities
FastEthernet6/3	
Model:	WS-X4232-GB-RJ-RJ-45
Type:	10/100BaseTX
Speed:	10,100,auto
Duplex:	half,full,auto
Auto-MDIX	yes
Trunk encap. type:	802.1Q,ISL
Trunk mode:	on,off,desirable,nonegotiate
Channel:	yes
Broadcast suppression:	percentage(0-100), hw
Flowcontrol:	<pre>rx-(none),tx-(none)</pre>
VLAN Membership:	static, dynamic
Fast Start:	yes
Queuing:	<pre>rx-(N/A), tx-(1p3q1t, Sharing/Shaping)</pre>
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
Maximum MTU:	1552 bytes (Baby Giants)
Multiple Media Types:	no
Diagnostic Monitoring:	N/A
Switch#	

Related Commands

Command	Description				
show interfaces counters	Displays the traffic on the physical interface.				

show interfaces counters

To display the 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	(Optio	nal) Displa	ys all the int	erface coun	ters incluc	ling errors	s, trunk, and deta	.il.
	detail	(Optio	(Optional) Displays the detailed interface counters.						
	errors	(Optional) Displays the interface error counters.							
	storm-control	(Optional) Displays the number of packets discarded due to supprinterface.						suppression on th	ression on the
	trunk	(Optio	nal) Displa	ys the inter	face trunk c	ounters.			
	module mod	(Optio	nal) Limits	the display	to interface	es on a spe	cific mod	ule.	
Defaults	This command h	as no default	settings.						
Command Modes	Privileged EXEC	C mode							
Command History	Release Modification								
	12.1(8a)EWSupport 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	r the displa	y of total su	ppression d	iscards.			
Usage Guidelines	If you do not ent The display for t					-	-		
Examples	This example sh	ows how to d	isplay the e	error counter	rs for a spec	ific modu	le:		
	Switch# show interfaces counters errors module 1								
	Port Al: Gi1/1 Gi1/2	ign-Err F 0 0	CS-Err 2 0 0	Kmit-Err 0 0	Rcv-Err U 0 0	nderSize 0 0			
	Port Sing	le-Col Multi	-Col Late	e-Col Exces	s-Col Carr	i-Sen	Runts	Giants	
	Gi1/1	0	0	0	0	0	0	0	
	Gi1/2 Switch#	0	0	0	0	0	0	0	
	DWT CCII#								
This example shows how to display the traffic that is 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
Port Gi1/1	OutOctets O	OutUcastPkts 0	OutMcastPkts 0	OutBcastPkts 0
			OutMcastPkts 0 0	OutBcastPkts 0 0

This example shows how to display the 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 that are discarded due to suppression:

Switch# show interfaces counters storm-control

Multicast Suppression : Enabled

Port	BcastSuppLevel	TotalSuppressionDiscards
Fa5/35	10.00%	6278550
Switch#		

Related Commands	Command	Description
	show interfaces capabilities	Displays the interface capabilities for an interface or for all
		the interfaces on a switch.

show interfaces description

To display a description and status of an interface, use the show interfaces description command.

show interfaces [interface] description

Syntax Description	interface (Optional) Type of interface. This command has no default settings.				
Defaults					
Command Modes	Privileged EX	KEC mode			
Command History	Release	Modific	ation		
	12.1(8a)EWSupport for this command was introduced on the Catalyst 4500 series switch.				
Examples	This example	shows how t	o display i	nformation for all interfaces:	
		v interfaces	_		
	Interface S		_	ion DI Description First interface	
	Interface S PO0/0 a	Status	Protoco	ol Description	
	Interface S POO/0 a POO/1 a	Status admin down	Protoco down	ol Description	
Related Commands	Interface S PO0/0 a PO0/1 a Gi1/1 u	Status admin down admin down	Protoco down down	Dl Description First interface	

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_n</i>	<i>um</i> (Optional) Limits the display to interfaces on a module.
Syntax Description	module mod_n	(Optional) Emitts the display to interfaces on a module.
Defaults	This command	has no default settings.
Command Modes	Privileged EXE	C mode
Command History	Release	Modification
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Usage Guidelines		state is up, the command displays 0:00. If the interface state is down, the time (in hours, conds) is displayed.
Examples	-	hows how to display active link-level information:
	Port Name Gi1/1 Gi1/2 Gi3/1 Gi3/2 Fa4/1 Fa4/2 Fa4/3 Fa4/4	Down Time 00:00:00 00:00:00 00:00:00 00:00:00 00:00:00 00:00:00 00:00:00 00:00:00 00:00:00
	This example sl	hows how to display inactive link-level information:
	Switch# show i	interfaces link
	Port Name Gi3/4 Gi3/5 Gi3/6 Gi4/1	Down Time 1 minute 28 secs 1 minute 28 secs 1 minute 28 secs 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 mod	(Optional) Limits the display to interfaces on a specific module.		
Defaults	This command has no default settings.			
Command Modes	EXEC			
Command History	Release	Modification		
Examples	12.1(13)EW This example a	Support for this command was introduced on the Catalyst 4500 series switch.		
Examples	This example :			
Examples	This example : Switch> show Port Name	shows how to display the MTU size for all interfaces on module 1: interfaces mtu module 1 MTU		
Examples	This example : Switch> show Port Name Gi1/1	shows how to display the MTU size for all interfaces on module 1: interfaces mtu module 1 MTU 1500		
Examples	This example : Switch> show Port Name	shows how to display the MTU size for all interfaces on module 1: interfaces mtu module 1 MTU		
Examples Related Commands	This example : Switch> show Port Name Gi1/1 Gi1/2	shows how to display the MTU size for all interfaces on module 1: interfaces mtu module 1 MTU 1500		

show interfaces private-vlan mapping

To display PVLAN mapping information for VLAN SVIs, use the **show interfaces private-vlan mapping** command.

show interfaces private-vlan mapping [active]

Syntax Description	active	(Optiona	1) Displays active interfaces only.
Defaults	This comm	and has no	default settings.
Command Modes	Privileged	EXEC mode	
Command History	Release	Мо	lification
	12.1(8a)EV	V Sup	port for this command was introduced on the Catalyst 4500 series switch.
Examples	This examp	le shows ho	ow to display PVLAN mapping information:
Lxampies	Switch# sh		ces private-vlan mapping
	vlan2 Switch#	301 302	isolated isolated
Related Commands	Command		Description
	private-vla	an	Configures private VLANs and the association between a private VLAN and a secondary VLAN.
	private-vla	an mapping	

show interfaces status

To display the interface status or a list of interfaces in error-disabled state, use the **show interfaces status** command.

show interfaces status [err-disabled | inactive] [module {module }]

Syntax Description	err-disabled	(Optional) Displays interfaces in error-disabled state.	-
	inactive	(Optional) Displays interfaces in inactive state.	•
	module module	(Optional) Displays interfaces on a specific module.	•
			•
Defaults	This command has no	default settings.	

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(40)SG	Support for WS-X4606-10GE-E Twin Gigabit convertor introduced.

Examples

This example shows how to display the status of all interfaces:

Switch# show interfaces status

Port	Name	Status	Vlan	Duplex	Speed	Туре
Gi1/1		disabled	routed	full	1000	missing
Gi1/2		notconnect	1	full	1000	unknown (4)
Fa5/1		disabled	routed	auto	auto	10/100BaseTX
Fa5/2		disabled	routed	auto	auto	10/100BaseTX
Fa5/3		disabled	routed	auto	auto	10/100BaseTX
Fa5/4		disabled	routed	auto	auto	10/100BaseTX
Fa5/15		disabled	routed	auto	auto	10/100BaseTX
Fa5/16		disabled	routed	auto	auto	10/100BaseTX
Fa5/17		disabled	routed	auto	auto	10/100BaseTX
Switch#						

This example shows how to display the status of interfaces in an error-disabled state:

Switch# show interfaces status err-disabled

Port Name Status Reason Fa9/4 notconnect link-flap

informational error message when the timer expires on a cause

 $5d04h:\PM-SP-4-ERR_RECOVER:\Attempting to recover from link-flap err-disable state on Fa9/4 Switch#$

This example shows how to display the Gigabit Ethernet interfaces on a WS-X4606-10GE-E using the TwinGig Convertor:

Switch# show interfaces status module 1 Port Name Status Vlan Duplex Speed Type Te1/1 inactive 1 full 10G No X2 Te1/2 inactive 1 full 10G No X2 Te1/3 inactive 1 full 10G No X2 Tel/4 notconnect 1 full 10G No X2 Tel/5 notconnect 1 full 10G No X2 Te1/6 notconnect 1 full 10G No X2 Gi1/7 notconnect 1 full 1000 No Gbic Gi1/8 notconnect 1 full 1000 No Gbic Gi1/9 notconnect 1 full 1000 No Gbic Gi1/10 notconnect 1 full 1000 No Gbic Gi1/11 notconnect 1 full 1000 No Gbic Gi1/12 notconnect 1 full 1000 No Gbic Gi1/13 inactive 1 full 1000 No Gbic Gi1/14 inactive 1 full 1000 No Gbic Gi1/15 inactive 1 full 1000 No Gbic Gi1/16 inactive 1 full 1000 No Gbic Gi1/17 inactive 1 full 1000 No Gbic Gi1/18 inactive 1 full 1000 No Gbic Switch#

Related Commands Co

Command	Description		
errdisable detect	Enables error-disable detection.		
hw-module port-group	Selects either Gigabit Ethernet or Ten Gigabit Ethernet interfaces on your module.		
show errdisable recovery	Displays error disable recovery timer information.		

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	interface-id	(Optional) Interface ID for the physical port.					
	module mod(Optional) Limits the display to interfaces on the specified module; valid values are from 1 to 6.						
Defaults	This command I	has no default settings.					
command Modes	Privileged EXE	C mode					
Command History	Release	Modification					
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.					
	12.1(19)EW	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.					
	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 Pruning VLANs						
	Name:Gi1/2 Switchport:Ena	bled					

```
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 f3/1 switchport
show interface f3/1 switchport
Name: Fa3/1
Switchport: Enabled
Administrative Mode: private-vlan trunk promiscuous
Operational Mode: private-vlan trunk promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: 1
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dotlq
Administrative private-vlan trunk normal VLANs: 1
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings:
    10 (VLAN0010) 100 (VLAN0100)
Operational private-vlan:
  10 (VLAN0010) 100 (VLAN0100)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Unknown unicast blocked: disabled
```

Unknown multicast blocked: disabled Unknown multicast blocked: disabled Appliance trust: none Switch#

Related Commands	Command	Description		
	show interfaces capabilities	Displays the interface capabilities for an interface or for all the interfaces on a switch.		
	show interfaces counters	Displays the traffic on the physical interface.		

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	int_name	(Optional) 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 mod	(Optional) Limits the display to interfaces on a specific module.
Defaults	The noninterfac	e-specific versions of the show interfaces transceiver command are enabled by default.
	a transceiver (G	becific versions of these commands are enabled by default if the specified interface has BIC or SFP) that is configured for diagnostic monitoring, and the transceiver is in a ports diagnostic monitoring.
Command Modes	Privileged EXE	C mode
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		
Usage Guidelines	• At least one	faces transceiver command provides useful information under the following conditions: e transceiver is installed on a chassis that is configured for diagnostic monitoring. iver is in a module that supports diagnostic monitoring.

confirm.

Examples

This example shows how to display diagnostic monitoring data for all interfaces with transceivers installed on the switch:

Switch# show interfaces transceiver

++ : hig NA or N/	ce is external gh alarm, + : /A: not applic liamperes, dBm	high war able, Tx:	ning, - : transmit,	low warni Rx: recei	ng, :	-
	_			Optical	Optical	
	Temperature	Voltage	Current	Tx Power	Rx Power	
Port	(Celsius)	(Volts)	(mA)	(dBm)	(dBm)	
 Gi1/1	48.1	3.30	0.0	0 1		
GII/I	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	
witch#						

Switch#



Note The value for the 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 the Tx Power or the 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.

	Temperature (Celsius)	(Celsius)	Threshold	Threshold (Celsius)	Threshold (Celsius)
		100.0			
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
		High Alarm	High Warn	Low Warn	Low Alarm
	Voltage	Threshold	Threshold	Threshold	Threshold
Port	(Volts)	. ,	(Volts)	, ,	. ,
Gi1/1		6.50			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
	Current	High Alarm Threshold	-		
Port	(milliamperes)		(mA)		
	0.0	130.0			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

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)	Threshold	Low Alarm Threshold (dBm)
Gi1/1	N/A	8.1	8.1	N/A	N/A
Gi1/1 Gi1/2	-30.9	8.1	8.1	N/A N/A	N/A N/A
	N/A (-28.5)	5.9	-6.7	-28.5	
Gi2/1 Gi2/2	N/A (-19.5)	5.9	-6.7	-28.5	
itch#					

Switch#

This example shows how to display the 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).

				Optical	Optical
	Temperature	Voltage	Current	Tx Power	Rx Power
Port	(Celsius)	(Volts)	(mA)	(dBm)	(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 the 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)	Threshold	Threshold (mA)	Threshold (mA)
 Gi2/1	50.6 +	60.0			
Gi2/2	25.8	60.0	40.0	10.0	5.0
Port	Optical Transmit Power (dBm)	Threshold	Threshold	Threshold	Threshold
	-16.7 (-13.0)				
Gi2/2	0.8 (5.1)	3.4	3.2	-0.3	-0.5
	Optical Receive Power	Threshold	Threshold	Threshold	Threshold
Port	(dBm)	(dBm)			(dBm)
Gi2/1	N/A (-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 the 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).
```

				Optical	Optical
	Temperature	Voltage	Current	Tx Power	Rx Power
Port	(Celsius)	(Volts)	(mA)	(dBm)	(dBm)
Gi2/1	43.7	5.03	50.6 +	-16.7	N/A
Switch#					

This example shows how to display detailed the 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

Port	Current (milliamperes)	High Alarm Threshold (mA)	Threshold	Threshold	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)	Threshold	Threshold	Threshold
Gi2/1	-16.7 (-13.0)	3.4	3.2	-0.3	-0.5
Port	Optical Receive Power (dBm)	High Alarm Threshold (dBm)	5		Low Alarm Threshold (dBm)
Gi2/1 Switch#	N/A (-28.5)	5.9	-6.7	-28.5	-28.5

Related Commands	Command	Description	
	show idprom	Displays the IDPROMs for the chassis.	
	show interfaces status	Displays the interface status or a list of interfaces in error-disabled state.	

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		otional) Limits the d m 1 to 6.	lisplay to interfa	ces on the specified module; valid values are	
Defaults	This com	mand has no c	lefault settings.			
Command Modes	Privilege	d EXEC mode				
Command History	Release	Mod	ification			
	12.1(8a)	EW Supp	port for this comma	and was introduc	ced on the Catalyst 4500 series switch.	
Usage Guidelines	If you do	not specify a	keyword, only info	rmation for trun	iking ports is displayed.	
Examples	This exar	This example shows how to display interface-trunk information for module 5:				
	Switch#	show interfac	ces trunk module	5		
	Port Fa5/1 Fa5/2 Fa5/3	Mode routed routed routed	Encapsulation negotiate negotiate negotiate	Status routed routed routed	Native vlan 1 1	
	Fa5/4 Fa5/5 Fa5/6	routed routed off	negotiate negotiate negotiate	routed routed not-trunking	1 1 10	
	Fa5/7 Fa5/8 Fa5/9 Fa5/10	off off desirable desirable	negotiate negotiate n-isl negotiate	not-trunking not-trunking not-trunking	10 1 1 1	
	Fa5/11 Fa5/12	routed routed	negotiate negotiate	routed routed	1 1	
	 Fa5/48	routed	negotiate	routed	1	
	Port Fa5/1 Fa5/2 Fa5/3 Fa5/4 Fa5/5 Fa5/6 Fa5/7	none none none none none none	ved on trunk			
	Fa5/8 Fa5/9	200 1-1005				

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
02,850,91	7,999,1002-1005
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
Fa5/9 02,850,91	1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8 7,999,1002-1005
	1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8 7,999,1002-1005 none
02,850,91	7,999,1002-1005
02,850,91 Fa5/10	7,999,1002-1005 none
02,850,91 Fa5/10	7,999,1002-1005 none
02,850,91 Fa5/10	7,999,1002-1005 none
02,850,91 Fa5/10 Fa5/11	7,999,1002-1005 none none
02,850,91 Fa5/10 Fa5/11 Fa5/48	7,999,1002-1005 none none
02,850,91 Fa5/10 Fa5/11 Fa5/48 Switch#	7,999,1002-1005 none none
02,850,91 Fa5/10 Fa5/11 Fa5/48 Switch# This exam	none none none none
02,850,91 Fa5/10 Fa5/11 Fa5/48 Switch# This exam	7,999,1002-1005 none none
02,850,91 Fa5/10 Fa5/11 Fa5/48 Switch# This exam	none none none none

Fa5/9 desirable n-isl trunking 1 Vlans allowed on trunk Port Fa5/9 1-1005 Vlans allowed and active in management domain Port 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 Vlans in spanning tree forwarding state and not pruned Port 1-6, 10, 20, 50, 100, 152, 200, 300, 303-305, 349-351, 400, 500, 521, 524, 570, 801-8 Fa5/9 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	statistic	S	have been		s for the following types of packets th feature: forwarded, dropped, MAC idation failure.
	vlan vla	in-range	statistics keyword,	for the selected ran	he statistics keyword, displays the ge of VLANs. Without the statistics uration and operating state of DAI for
	interfac	:es interface-name	the provid command	led interface. When	state and the rate limit of ARP packets to the interface name is not specified, state and rate limit for all applicable
efaults	This con	nmand has no defa	ult settings.		
ommand Modes	Privilege	ed EXEC mode			
Command History	Release	Modific	ation		
ommand History	Release 12.1(19)			and was introduced	I on the Catalyst 4500 series switch.
	This exa VLAN 3)EW Support mple shows how to :	for this comm o display the st	atistics of packets	d on the Catalyst 4500 series switch.
	This exa VLAN 3 Switch#)EW Support mple shows how to : show ip arp insp	for this comm o display the st pection static	atistics of packets a	that have been processed by DAI for
	This exa VLAN 3)EW Support mple shows how to :	for this comm o display the st	atistics of packets	
	This exa VLAN 3 Switch#)EW Support mple shows how to : show ip arp insp Forwarded 	for this comm o display the st pection statis Dropped	atistics of packets stics vlan 3 DHCP Drops	ACL Drops
	This exa VLAN 3 Switch# Vlan 3	DEW Support mple shows how to : show ip arp insp Forwarded 	for this comm o display the st pection statis Dropped 102407	atistics of packets a stics vlan 3 DHCP Drops 102407	ACL Drops
command History	This exa VLAN 3 Switch# Vlan 3 Vlan 	DEW Support mple shows how to : show ip arp insp Forwarded 	for this comm o display the st pection statis Dropped 102407 ACL Permits 	atistics of packets a stics vlan 3 DHCP Drops 102407 Source MAC Fail	ACL Drops

This example shows how to display the statistics of packets that have been processed by DAI for all active VLANs:

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 Fa	ailures
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 Failur		tion 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#				

Switch# show ip arp inspection statistics

This example shows how to display the configuration and operating state of DAI for VLAN 1:

```
Switch# show ip arp inspection vlan 1 % \left( {{{\bf{n}}_{{\rm{n}}}} \right)
Source Mac Validation : Disabled
Destination Mac Validation : Disabled
IP Address Validation : Disabled
      Configuration Operation ACL Match Static ACL
Vlan
        -----
                       -----
 ____
                                                    _____
        Enabled
                     Active
   1
        ACL Logging DHCP Logging
Vlan
 ____
  1
        Deny
                       Deny
Switch#
```

This example shows how to display the trust state of Fast Ethernet interface 6/1:

Switch# show ip arp inspection interfaces fastEthernet 6/1 Interface Trust State Rate (pps) Burst Interval ----- -----_____ Untrusted 20 5 Fa6/1 Switch#

This example shows how to di	isplay the trust state of the	interfaces on the switch:
------------------------------	-------------------------------	---------------------------

Switch# show ip Interface	arp inspection Trust State	interfaces 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

Command	Description
arp access-list	Defines an ARP access list or adds clauses at the end of a predefined list.
clear ip arp inspection log	Clears the status of the log buffer.
show ip arp inspection log	Displays the status of the log buffer.

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 mode

 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	1.1.11	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	Command	Description
	arp access-list	Defines an ARP access list or adds clauses at the end of a predefined list.
	clear ip arp inspection log	Clears the status of the log buffer.

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	vlan_num	Number of the VLAN.			
	detail	(Optional) Displays detailed information.			
Defaults	This commar	nd has no default settings.			
ommand Modes	Privileged EX	XEC mode			
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# Switch# FastEthernet3/3				
	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 Ta Switch#	able has 5 adjacencies			

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 mode

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(25)EWA	Support for option 82 on untrusted ports was added.

Examples	This example shows how to display the DHCP snooping configuration:

mproo	This example shows now to display the Difer shooping configuration.
	Switch# show ip dhcp snooping
	Switch DHCP snooping is enabled
	DHCP snooping is configured on following VLANs:
	500,555
	DHCP snooping is operational on following VLANs:
	500,555
	DHCP snooping is configured on the following L3 Interfaces:
	Insertion of option 82 is enabled
	circuit-id default format: vlan-mod-port
	remote-id: switch123 (string)
	Option 82 on untrusted port is not allowed Verification of hwaddr field is enabled DHCP
	snooping trust/rate is configured on the following Interfaces:
	Interface Trusted Rate limit (pps)
	 FastEthernet5/1 ves 100
	Custom circuit-ids:
	VIAN 55: customer-555
	FastEthernet2/1 no unlimited
	Custom circuit-ids:
	VLAN 500: customer-500
	Switch#

Related Commands	Command	Description		
	ip dhcp snooping	Globally enables DHCP snooping.		
ip dhcp snooping information option		Enables DHCP option 82 data insertion.		
	ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.		

Command	Description
ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.

show ip dhcp snooping binding

To display the 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]

	n ip-address	(Op	ptional) IP address for th	e binding entrie	es.	
	mac-address	(Op	(Optional) MAC address for the binding entries.			
	vlan <i>vlan_num</i>	-	otional) Specifies a VLA			
	interface interf	face_num (Op	otional) Specifies an inte	rface.		
Defaults	If no argument i	is specified, the sv	vitch will display the ent	tire DHCP snot	pping binding table.	
Command Modes Privileged EXEC mode						
Command History	Release	Modification				
	12.1(12c)EW	Support for thi	s command was introduc	ced on the Cata	lyst 4500 series switch.	
Examples	range.		use the optional <i>last_vlas</i> ay the DHCP snooping b	-		
-	range.	nows how to displa	-	-		
Switch# show ip MacAddress	This example sh	nows how to displa	ay the DHCP snooping b	inding entries t		
Switch# show ip MacAddress 0000.0100.0201	This example sh	nows how to displa ling ase (seconds)	ay the DHCP snooping b	inding entries t	for a switch:	
MacAddress 0000.0100.0201 Switch# Switch# show ip	range. This example sh dhcp snooping bind IP Address Lea 10.0.0.1	nows how to displa ding ase (seconds) 1600 nows how to displa ding 172.100.101	ay the DHCP snooping b Type dhcp-snooping ay an IP address for DHC 102	vLAN Inte 100	For a switch: rface FastEthernet3/1 nding entries:	
Switch# show ig MacAddress 0000.0100.0201 Switch#	range. This example sh dhcp snooping bind IP Address Lea 10.0.0.1	nows how to displa fing ase (seconds) 1600 nows how to displa	ay the DHCP snooping b Type dhcp-snooping ay an IP address for DHC 102 Type	vLAN Inte 100	For a switch: rface FastEthernet3/1	

This example shows how to display the MAC address for the DHCP snooping binding entries:

Switch# show ip dhcp snooping binding 55.5.5.2 0002.b33f.3d5f

MacAddress	IpAddress	Lease(sec)	Туре	VLAN Interface
00:02:B3:3F:3D:5F Switch#	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)	Туре	VLAN	Interface
00:02:B3:3F:3D:5F Switch#	55.5.5.2	479	dhcp-snooping	99	FastEthernet6/36

This example shows how to display the dynamic DHCP snooping binding entries:

Switch# show ip dhcp snooping binding dynamic

MacAddress	IP Address	Lease (seconds)	Туре	VLAN	Interface
0000.0100.0201	10.0.0.1	1600	dhcp-snooping	100	FastEthernet3/1
Switch#					

This example shows how to display the DHCP snooping binding entries on VLAN 100:

Switch# show ip dhcp snooping binding vlan 100'

MacAddress	IP Address	Lease (seconds)	Туре	VLAN	Interface
0000.0100.0201 Switch#	10.0.0.1	1600	dhcp-snooping	100	FastEthernet3/1

This example shows how to display the DHCP snooping binding entries on Ethernet interface 0/1:

${\tt Switch} \#$ show ip dhcp snooping binding interface fastethernet3/1

MacAddress	IP Address	Lease (seconds)	Туре	VLAN	Interface
0000.0100.0201	10.0.0.1	1600	dhcp-snooping	100	FastEthernet3/1

Table 2-19 describes the fields in the show ip dhcp snooping command output.

Table 2-19show ip dhcp snooping Command Output

Field	Description	
Mac Address	Client hardware MAC address.	
IP Address	ress Client IP address assigned from the DHCP server.	
Lease (seconds)	IP address lease time.	
Туре	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.	

Switch#

Related Commands Command Description Enables DHCP option 82 data insertion. ip dhcp snooping information option Configures the number of the DHCP messages that an ip dhcp snooping limit rate interface can receive per second. ip dhcp snooping trust Enables DHCP snooping on a trusted VLAN. Enables DHCP snooping on a VLAN or a group of VLANs. ip dhcp snooping vlan ip igmp snooping Enables IGMP snooping. ip igmp snooping vlan Enables IGMP snooping for a VLAN.

show ip dhcp snooping database

To display the status of the DHCP snooping database agent, use the **show ip dhcp snooping database** command.

show ip dhcp snooping database [detail]

Syntax Description	detail (Optional) Pro	vides ac	ditional operating s	tate and	statistics information.	
Defaults	This command h	ıas no default	setting	s.			
Command Modes	Privileged EXE	C mode					
Command History	Release	Modificati	on				
	12.1(12c)EW	Support fo	r this co	ommand was introdu	ced on	the Catalyst 4500 series switc	ch.
	12.1(19)EW			state and statistics in			
	Agent URL : Write delay Ti Abort Timer :		conds				
	Write delay Ti		conds				
	Agent Running : No						
	Delay Timer Expiry : Not Running Abort Timer Expiry : Not Running						
	Last Succeded						
	Last Failed Ti Last Failed Re		ilure :	recorded.			
	Total Attempts		0	Startup Failures		0	
	Successful Tra		0	Failed Transfers		0	
	Successful Rea		0	Failed Reads	:	0	
	Successful Wri		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 Succeded 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
                          0
Media Failures
                 :
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
Parse failures : 0
                                Unsupported vlans :
                                                         0
```

Switch#

Related Commands

Command	Description		
ip dhcp snooping	Globally enables DHCP snooping.		
ip dhcp snooping database	Stores the bindings that are generated by DHCP snooping.		
ip dhcp snooping information option	Enables DHCP option 82 data insertion.		
ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.		
ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.		
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.		

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 |
tengigabitethernet slot/port | null interface-number | vlan vlan_id]

fastethernet slot/port	(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.
tengigabitethernet <i>slot/port</i>	(Optional) Specifies the 10-Gigabit Ethernet interface and the number of the slot and port; valid values are from 1 to 2.
null interface-number	(Optional) Specifies the null interface and the number of the interface; the only valid value is 0 .
vlan vlan_id	(Optional) Specifies the VLAN and the number of the VLAN; valid values are from 1 to 4094.
If you do not specify	a VLAN, information for VLAN 1 is shown.
Privileged EXEC mo	ode
Release N	lodification
12.1(8a)EW S	upport for this command was introduced on the Catalyst 4500 series switch.
12.1(00)1.00	••
	dded support for extended VLAN addresses.
12.1(12c)EW A	dded support for extended VLAN addresses. dded support for the 10-Gigabit Ethernet interface.
12.1(12c)EW A 12.2(25)EW A	
12.1(12c)EWA12.2(25)EWAIf you omit the optic all interfaces.	dded support for the 10-Gigabit Ethernet interface.
-	gigabitethernet slot/port tengigabitethernet slot/port null interface-number vlan vlan_id If you do not specify Privileged EXEC mode Release M

Related Commands	Command	Description		
	clear ip igmp group	Deletes the IGMP group cache entries.		
	show ip igmp snooping mrouter	Displays information on the dynamically learned and manually configured multicast switch interfaces.		

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	profile number	(Optional) IGMP profile number to be displayed; valid ranges are from 1 to 4294967295.				
Defaults	This command ha	as no default settings.				
Command Modes	Privileged EXEC	mode				
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 num	ber is entered, all IGMP profiles are displayed.				
Examples	This example shows how to display IGMP profile 40:					
	IGMP Profile 40 permit	igmp profile 40 .1.1 233.255.255.255				
	This example shows how to display all IGMP profiles:					
	IGMP Profile 4 permit	<pre>igmp profile .9.0 230.9.9.0 .9.0 229.255.255.255</pre>				
Related Commands	Command	Description				

lelated Commands	Command	Description		
	ip igmp profile	Creates an IGMP profile.		

show ip igmp snooping

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 | groups | 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.					
-,	groups	(Optional) Specifies that the display will list VLAN members sorted by group IP addresses.					
	mrouter	(Optional) Specifies that the display will contain information on dynamically learn and manually configured multicast switch interfaces.					
	vlan vlan_id	un <i>vlan_id</i> (Optional) Specifies a VLAN; valid values are from 1 to 1001 and from 1006 to					
	a.b.c.d	Group or multicast IP 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.					
Command Modes	EXEC	Modification					
Command mistory		Woullication					
	$12.1(8_{0}) EW$	Support for this command was introduced on the Catalyst 4500 series switch					
	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.					
Usage Guidelines	12.1(19)EW 12.1(20)EW You can also u address table fo						

Examples

This example shows how to display the global snooping information on the switch:

Switch# show ip igmp snooping

Global IGMP Snooping conf	iguration:
	: Enabled : Enabled : Enabled : Disabled : 2
Vlan 1:	
IGMP snooping IGMPv2 immediate leave Explicit host tracking Multicast router learning CGMP interoperability mod	
Vlan 2:	
IGMP snooping IGMPv2 immediate leave Explicit host tracking Multicast router learning CGMP interoperability mod 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	2 v3	Fa3/15
Switch>			

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 2	224.0.1.40 224.2.2.2	v3 v3	Router 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	Туре	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 10 226.6.6.7VlanGroupVersion10226.6.6.7v3Fa7/13, Fa7/14Switch>
```

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>				

Γ

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
    _____
175.1.0.29INCLUDEstopped00:00:512175.2.0.30INCLUDEstopped00:04:142
```

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
                             : Fa7/13, Fa7/14
Member Ports
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>
```

Command **Related Commands**

ommands	Command	Description		
	ip igmp snooping	Enable IGMP snooping.		
	ip igmp snooping vlan immediate-leave	Enable IGMP immediate-leave processing.		
	ip igmp snooping vlan mrouter	Configures a Layer 2 interface as a multicast router interface for a VLAN.		
	ip igmp snooping vlan static	Configures a Layer 2 interface as a member of a group.		
	show ip igmp interface	Displays the information about the IGMP-interface status and configuration.		
	show ip igmp snooping mrouter	Displays information on the dynamically learned and manually configured multicast switch interfaces.		
	show mac-address-table multicast	Displays information about the multicast MAC address table.		
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 vlan_id	(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 a.b.c.d	(Optional) Specifies a reporter, source, or group IP address.
	group a.b.c.d	(Optional) Displays all members of a channel (source, group), sorted by interface or VLAN.
Defaults	This command has no defa	ault settings.
Command Modes	Privileged EXEC mode	
Command History	Release Modific	cation
	12.1(20)EW Support	t for this command was introduced on the Catalyst 4500 series switch.
	12.2(25)EW Added	support for the 10-Gigabit Ethernet interface.
Usage Guidelines	This command is valid onl	ly if explicit host tracking is enabled on the switch.
Examples	This example shows how t	to display host membership for the Gigabit Ethernet interface 4/1:
Examples	Switch# show ip igmp sn	to display host membership for the Gigabit Ethernet interface 4/1:
Examples	Switch# show ip igmp sn #channels: 5 #hosts : 1	ooping membership interface gigabitethernet4/1
Examples	Switch# show ip igmp sn #channels: 5 #hosts : 1	
Examples	Switch# show ip igmp sn #channels: 5 #hosts : 1 Source/Group Interface 1 40.40.40.2/224.10.10.10	ooping membership interface gigabitethernet4/1
Examples	Switch# show ip igmp sn #channels: 5 #hosts : 1 Source/Group Interface 1 40.40.40.2/224.10.10.10 40.40.40.4/224.10.10.10 Switch#	Reporter Uptime Last-Join Last-Leave Gi4/1 20.20.20.20 00:23:37 00:06:50 00:20:30
Examples	Switch# show ip igmp sn #channels: 5 #hosts : 1 Source/Group Interface 1 40.40.40.2/224.10.10.10 40.40.40.4/224.10.10.10 Switch# This example shows how t Switch# show ip igmp sn #channels: 5 #hosts : 1	wooping membership interface gigabitethernet4/1 Reporter Uptime Last-Join Last-Leave Gi4/1 20.20.20.20 00:23:37 00:06:50 00:20:30 Gi4/1 20.20.20.20 00:39:42 00:09:17 -

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	-	Uptime Last-Join/	Last-Leave	
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 snoopin Switch#	g membership	vlan 20		-	

Related Commands	Command	Description
	clear ip igmp snooping membership	Clears the explicit host tracking database.
	ip igmp snooping vlan explicit-tracking	Enables per-VLAN explicit host tracking.
	show ip igmp snooping	Displays information on dynamically learned and manually configured VLAN switch interfaces.

show ip igmp snooping mrouter

To display information on the 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 vlan-id (Optional)	Specifies a VI	LAN; valid values are from 1 to 1001 and from 1006 to 4094
Defaults	This command has no def	ault settings.	
Command Modes	Privileged EXEC mode		
Command History	Release Modifie	cation	
	12.1(8a)EW Suppor	rt for this comm	nand was introduced on the Catalyst 4500 series switch.
	12.1(19)EW Added	support for ext	tended VLAN addresses.
Usage Guidelines	address table for a VLAN	that has IGMF ooping informa	-table multicast command to display entries in the MAC P snooping enabled. ation for the VLAN interfaces by entering the show ip igmp
	address table for a VLAN You can display IGMP sno interface vlan vlan-num c	that has IGMF ooping informa command. to display snoo	P snooping enabled. ation for the VLAN interfaces by entering the show ip igmp oping information for a specific VLAN:
	address table for a VLAN You can display IGMP sno interface vlan vlan-num of This example shows how to Switch# show ip igmp sn vlan ports	that has IGMF ooping informa command. to display snoo	P snooping enabled. ation for the VLAN interfaces by entering the show ip igmp oping information for a specific VLAN: er vlan 1
Examples	address table for a VLAN You can display IGMP sno interface vlan vlan-num of This example shows how to Switch# show ip igmp sn vlan ports 1 Gil/1,Gi2/	that has IGMF ooping informa command. to display snoo	P snooping enabled. ation for the VLAN interfaces by entering the show ip igmp oping information for a specific VLAN: er vlan 1
Examples	address table for a VLAN You can display IGMP sno interface vlan vlan-num of This example shows how for Switch# show ip igmp sn vlan ports 1 Gi1/1,Gi2/ Switch#	that has IGMF ooping informa command. to display snoo hooping mroute (1,Fa3/48,Swit	P snooping enabled. ation for the VLAN interfaces by entering the show ip igmp oping information for a specific VLAN: er vlan 1
Usage Guidelines Examples Related Commands	address table for a VLAN You can display IGMP sno interface vlan vlan-num of This example shows how to Switch# show ip igmp sn vlan ports 1 Gil/1,Gi2/ Switch# Command	that has IGMF ooping informa command. to display snoo hooping mroute (1,Fa3/48,Swit	P snooping enabled. ation for the VLAN interfaces by entering the show ip igmp oping information for a specific VLAN: er vlan 1

show ip igmp snooping vlan

To display information on the 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	vlan_num N	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	C mode			
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 Examples	address table for	e the show mac-address-table multicast command to display the entries in the MAC a VLAN that has IGMP snooping enabled.			
•	Switch# show ip igmp snooping vlan 2 vlan 2				
	IGMP snooping (IGMP snooping (IGMP snooping (IGMP snooping (IGMP snooping (is globally enabled TCN solicit query is globally enabled global TCN flood query count is 2 is enabled on this Vlan immediate-leave is disabled on this Vlan mrouter learn mode is pim-dvmrp on this Vlan is running in IGMP_ONLY mode on this Vlan			

Related Commands C

Command	Description
ip igmp snooping	Enable IGMP snooping.
ip igmp snooping vlan immediate-leave	Enable IGMP immediate-leave processing.
ip igmp snooping vlan mrouter	Statically configures a Layer 2 interface as a multicast router interface for a VLAN.
ip igmp snooping vlan static	Configures a Layer 2 interface as a member of a group.
show ip igmp interface	Displays the information about the IGMP-interface status and configuration.
show ip igmp snooping mrouter	Displays information on the dynamically learned and manually configured multicast switch interfaces.
show mac-address-table multicast	Displays information about the multicast MAC address table.

show ip interface

To display the usability status of interfaces that are configured for IP, use the **show ip interface** command.

show ip interface [type number]

Syntax Description	type	(Optional) Interface type.	
	number	(Optional) Interface number.	
Defaults	This command	has no default settings.	
Command Modes	EXEC		
Command History	Release	Modification	
	12.2(25)EW	Extended to include the 10-Gigabit Ethernet interface.	
Usage Guidelines	interface is usa If the software from the routin determine back	software automatically enters a directly connected route in the routing table if the able. A usable interface is one through which the software can send and receive packets. determines that an interface is not usable, it removes the directly connected routing entry ag table. Removing the entry allows the software to use dynamic routing protocols to cup routes to the network, if any.	
		can provide two-way communication, the line protocol is marked "up." If the interface able, the interface is marked "up."	
	If you specify an optional interface type, you see information only on that specific interface.		
	If you specify no optional arguments, you see information on all the interfaces.		
	fast switching	chronous interface is encapsulated with PPP or Serial Line Internet Protocol (SLIP), IP is enabled. The show ip interface command on an asynchronous interface that is <i>v</i> ith PPP or SLIP displays a message indicating that IP fast switching is enabled.	
Examples	This example s	shows how to display the usability status for a specific VLAN:	
	Vlan1 is up, Internet ad Broadcast a Address det MTU is 1500 Helper addr Directed br Outgoing ac	ress is not set roadcast forwarding is disabled rcess list is not set rcess list is not set	

```
Local Proxy ARP is disabled
 Security level is default
 Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
 ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
 IP Fast switching turbo vector
 IP Normal CEF switching turbo vector
 IP multicast fast switching is enabled
 IP multicast distributed fast switching is disabled
 IP route-cache flags are Fast, CEF
 Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
 Network address translation is disabled
  WCCP Redirect outbound is disabled
 WCCP Redirect inbound is disabled
 WCCP Redirect exclude is disabled
 BGP Policy Mapping is disabled
  Sampled Netflow is disabled
  IP multicast multilayer switching is disabled
 Netflow Data Export (hardware) is enabled
Switch#
```

Table 2-20 describes the fields that are shown in the example.

Field	Description	
Ethernet0 is up	If the interface hardware is usable, the interface is marked "up." For an interface to be usable, both the interface hardware and line protocol must be up.	
line protocol is up	If the interface can provide two-way communication, the line protocol is marked "up." For an interface to be usable, both the interface hardware and line protocol must be up.	
Internet address and subnet mask	IP address and subnet mask of the interface.	
Broadcast address	Broadcast address.	
Address determined by	Status of how the IP address of the interface was determined.	
MTU	MTU value that is set on the interface.	
Helper address	Helper address, if one has been set.	
Secondary address	Secondary address, if one has been set.	
Directed broadcast forwarding	Status of directed broadcast forwarding.	
Multicast groups joined	Multicast groups to which this interface belongs.	
Outgoing access list	Status of whether the interface has an outgoing access list set.	
Inbound access list	Status of whether the interface has an incoming access list set.	

Table 2-20show ip interface Field Descriptions

Field	Description
Proxy ARP	Status of whether Proxy Address Resolution Protocol (ARP) is enabled for the interface.
Security level	IP Security Option (IPSO) security level set for this interface.
Split horizon	Status of split horizon.
ICMP redirects	Status of the redirect messages on this interface.
ICMP unreachables	Status of the unreachable messages on this interface.
ICMP mask replies	Status of the mask replies on this interface.
IP fast switching	Status of whether fast switching has been enabled for this interface. Fast switching is typically enabled on serial interfaces, such as this one.
IP SSE switching	Status of the IP silicon switching engine (SSE).
Router Discovery	Status of the discovery process for this interface. It is typically disabled on serial interfaces.
IP output packet accounting	Status of IP accounting for this interface and the threshold (maximum number of entries).
TCP/IP header compression	Status of compression.
Probe proxy name	Status of whether the HP Probe proxy name replies are generated.
WCCP Redirect outbound is enabled	Status of whether packets that are received on an interface are redirected to a cache engine.
WCCP Redirect exclude is disabled	Status of whether packets that are targeted for an interface are excluded from being redirected to a cache engine.
Netflow Data Export (hardware) is enabled	NDE hardware flow status on the interface.

 Table 2-20
 show ip interface Field Descriptions (continued)

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 nonzero counters shown.			
	log (Optional) Specifies a log of the most recent number of MFIB-related events. The recent event is first.			
	n	(Optional) Number of events.		
Defaults	This comman	nd has no default settings.		
Command Modes	Privileged EX	KEC mode		
Command History	Release	Modification		
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.		
	12.2(40)SG	Support for command introduced on the Supervisor Engine 6-E and Catalyst 4900M chassis.		
Usage Guidelines	-	isor Engine 6-E and Catalyst 4900M chassis, the output of the show ip mfib command does ny hardware counters.		
	The MFIB tal	ble contains a set of IP multicast routes; each route in the MFIB table contains several flags 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. These 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.			
	the C flag	ed (C) flag—When set on a route, the C flag has the same meaning as the S flag, except that g indicates that only packets sent by directly connected hosts to the route should be signaled ocol process.		

Examples

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 the ingress packets should be treated and whether packets matching the route should be forwarded onto interface 1. These per-interface flags are associated with the 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 with the A flag as described above. The set of forwarding interfaces together form a multicast olist 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 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 4506 switch with Supervisor Engine III 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.

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

Command	Description
clear ip mfib counters	Clears the global MFIB counters and the counters for all active MFIB routes.

show ip mfib fastdrop

L

To display 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 mode **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 fasttdrop 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	Command	Description	
	clear ip mfib fastdrop	Clears all the MFIB fast-drop entries.	

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	interface_type slot/port	(Optional) Interface type and number of the slot and port; valid values for <i>interface type</i> are fastethernet , gigabitethernet , tengigabitethernet , null , and vlan .				
	host_name	(Optional) Name or IP address as defined in the DNS hosts table.				
	host_address source	(Optional) IP address or name of a multicast source.				
	active	(Optional) Displays the rate that active sources are sending to multicast groups.				
	kbps interface_type num	(Optional) Minimum rate at which active sources are sending to multicastgroups; active sources sending at this rate or greater will be displayed. Valid values are from 1 to 4294967295 kbps.				
	count	(Optional) Displays the route and packet count information.				
	pruned	(Optional) Displays the pruned routes.				
	static	(Optional) Displays the static multicast routes.				
	summary	(Optional) Displays a one-line, abbreviated summary of each entry in the IP multicast routing table.				
Command Modes	Privileged EXEC n					
Command History		Modification				
		Support for this command was introduced on the Catalyst 4500 series switch.				
	12.2(25)EW	Added support for the 10-Gigabit Ethernet interface.				
Usage Guidelines		optional arguments and keywords, the show ip mroute command displays all the alticast routing table.				
	The show ip mrout to <i>kbps</i> .	The show ip mroute active <i>kbps</i> command displays all the sources sending at a rate greater than or equal to <i>kbps</i> .				
	entries. The star re- refers to the destina	ing table is populated by creating source, group (S,G) entries from star, group $(*,G)$ fers to all source addresses, the "S" refers to a single source address, and the "G" ation multicast group address. In creating (S,G) entries, the software uses the best path group found in the unicast routing table (through Reverse Path Forwarding (RPF).				

Switch# show ip mroute active

Examples	This example shows how to display all the entries in the IP multicast routing table:
	Switch# show ip mroute
	<pre>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</pre>
	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
	<pre>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</pre>
	(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 the active sources are sending to the multicast groups and to display only the active sources that are sending at greater than the default rate:

```
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(lsec), 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(lsec), 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(lsec), 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#

Table 2-21 describes the fields shown in the output.

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 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; indicates if the software is registered for a multicast source.
T - SPT-bit set	Status of the packets; indicates if the packets been received on the shortest path source tree.

Table 2-21 show ip mroute Field Descriptions

Field	Description
J - Join SPT	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 0 kbps.) 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.
	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.
	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.
	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.
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)	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.
	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 comma G" entries. (*,G) entries are used to build (S,G) entries.
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.

 Table 2-21
 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 indicates that the group is using the static-map virtual circuit.		
Forward/Dense	Status of the packets; indicates if they 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.		

Table 2-21	show ip mroute Field Descriptions (continued)
	· · · · · · · · · · · · · · · · · · ·

Related Commands	Command	Description
	ip multicast-routing (refer to Cisco IOS documentation)	Enables IP multicast routing.
	ip pim (refer to Cisco IOS documentation)	Enables Protocol Independent Multicast (PIM) on an interface.

show ip source binding

To display IP source bindings that are 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		al) Binding IP a	1) Binding IP address.			
	mac-address	(Option	al) Binding MA	C address.			
	dhcp-snooping	(Option	al) DHCP-snoo	ping type bind	ling.		
	static	(Option	al) Statically co	nfigured bind	ing.		
	vlan vlan-id(Optional) VLAN number.						
	interface interface-n	ame (Option	al) Binding inte	rface.			
Defaults	Displays both static a	nd DHCP snoopin	ng bindings.				
Command Modes	Privileged EXEC mod	de					
Command History	Release Modification						
	12.1(19)EWSupport for this command was introduced on the Catalyst 4500 series switch						
Usage Guidelines	The optional paramet	ers filter the disp	lay output resul	t.			
vamnlae	This axomple shows l	your to display the	ID source hind	nas			
xamples	This example shows l		P IP source bindi	ings:			
xamples	Switch# show ip sou MacAddress	irce binding IpAddress	Lease(sec)	ngs: Type		Interface	
Examples	Switch# show ip sou	urce binding	Lease(sec)	-		Interface FastEthernet6/10	
xamples	Switch# show ip sou MacAddress	arce binding IpAddress	Lease(sec)	Туре			
Examples	Switch# show ip sou MacAddress 00:00:00:0A:00:0B	IpAddress 11.0.0.1	Lease(sec) infinite	Type 	10	FastEthernet6/10	
Examples	Switch# show ip sou MacAddress 00:00:00:0A:00:0B Switch#	nrce binding IpAddress 11.0.0.1	Lease(sec) infinite e static IP bindin 0.0.1 0000.000	Type static	10 address 11 .c vlan 10 .0 interfa	FastEthernet6/10 .0.01: interface Fa6/10	

Related Commands	Command	Description
	ip source binding	Adds or deletes a static IP source binding entry.

show ip verify source

To display the 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 EXE	C mode				
Command History	Release	Modificatio				
	12.1(19)EW	Support for	this command	was introduced	on the Catalyst 4500) series switch.
Examples	interface with the source filte VLAN 10: Interface	the show ip ver cappears when r mode that is c Filter-type	ify source inte DHCP snoopir configured as II Filter-mode active	rface command: ng is enabled on ? P, and an existing IP-address	figuration and filters VLANs 10–20, inter g IP address binding Mac-address	face fa6/1 has IP 10.0.0.1 is on Vlan
	• This output snooping is as IP, and the Interface	appears when enabled on VI here is an exist Filter-type	d VLANs that you enter the sh ANs 10–20, ir ing IP address Filter-mode	do not have a val now ip verify sound terface fa6/1 has binding 10.0.0.1 IP-address	s IP source filter mo	g. command and DHCP de that is configured Vlan
	-		•	how ip verify so abled for DHCP	ource interface fa6/	3 command and the
	Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
	fa6/3			snooping-vlan		

• This output appears when you enter the **show ip verify source interface fa6/4** command and the interface fa6/4 has an IP source filter mode that is configured as IP MAC and the 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	10.0.2	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

• This output appears when you enter the **show ip verify source interface fa6/5** command and the interface fa6/5 has IP source filter mode that is configured as IP MAC and existing IP MAC binding 10.0.0.3/aaaa.bbbb.ccce on VLAN 10, but port security is not enabled on fa6/5:

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
fa6/5 fa6/5	ip-mac ip-mac	active active	10.0.0.3 deny-all	permit-all permit-all	10 11-20

Note

Enable port security first because the DHCP security MAC filter cannot apply to the port or VLAN.

• This 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 that is configured:

DHCP security is not configured on the interface fa6/6.

This example shows how to display all the interfaces on the switch that have DHCP snooping security and IP Port Security tracking 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-tru	st-port		
Fa6/3	ip trk	active	40.1.1.24		10
Fa6/3	ip trk	active	40.1.1.20		10
Fa6/3	ip trk	active	40.1.1.21		10
fa6/4	ip-mac	active	10.0.2	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	Command	Description
	ip dhcp snooping information option	Enables DHCP option 82 data insertion.
	ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
	ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
	ip igmp snooping	Enables IGMP snooping.
	ip igmp snooping vlan	Enables IGMP snooping for a VLAN.
	ip source binding	Adds or deletes a static IP source binding entry.
	ip verify source	Enables IP source guard on untrusted Layer 2 interfaces.
	show ip source binding	Displays the DHCP snooping binding entries.

show ipc

To display IPC information, use the **show ipc** command. show ipc {nodes | ports | queue | status}

Syntax Description	nodes	Displays the participating nodes.
	ports	Displays the 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 mode

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 participating nodes:

Switch# show ipc nodes There are 3 nodes in this IPC realm.				
ID	Туре	Name	Last	Last
			Sent	Heard
10000	Local	IPC Master	C	0
2010000	Local	GALIOS IPC:Card 1	C	0
2020000	Ethernet	GALIOS IPC:Card 2	1	2 26
Switch#				

This example shows how to display the local IPC ports:

```
Switch# show ipc ports
There are 11 ports defined.
```

Port ID	Туре	Name	(curren	t/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 Po:	rt		
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:Con	ntrol		
2020000.4	unicast	GALIOS RFS :Standby			
2020000.5	unicast	Slave: Remote TTY Cl	ient Por	t	
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 ipv6 mld snooping

To display IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping configuration of the switch or the VLAN, use the **show ipv6 mld snooping** command.

show ipv6 mld snooping [vlan vlan-id]

Syntax Description	vlan vlan-id	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.
Command Modes	User EXEC mode	
Command History	Release	Modification
	12.2(40)SG	This command was introduced on the Catalyst 4500.
Usage Guidelines		to display MLD snooping configuration for the switch or for a specific VLAN. 02 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used
Examples	characteristics for a Switch> show ipv6	5 mld snooping vlan 100
	MLD snooping MLDv2 snooping (m	: Enabled minimal) : Enabled suppression : Enabled v : Disabled count : 2 ble : 3 ery count : 2
	Vlan 100: MLD snooping MLDv1 immediate 1 Explicit host tra Multicast router Robustness variab Last listener que Last listener que	acking : Enabled learning mode : pim-dvmrp ble : 3 ery count : 2
	This is an example	of output from the show ipv6 mld snooping command. It displays snooping all VLANs on the switch.
	Switch> show ipv6	

MLD snooping		Enabled
MLDv2 snooping (minimal)	:	Enabled
Listener message suppression	:	Enabled
TCN solicit query	:	Disabled
TCN flood query count	:	2
Robustness variable	:	3
Last listener query count	:	2
Last listener query interval	:	1000
Vlan 1:		
MLD snooping		: Disabled
MLDv1 immediate leave		: Disabled
Explicit host tracking		: Enabled
Multicast router learning mode	Э	: pim-dvmrp
Robustness variable		: 1
Last listener query count		: 2
Last listener query interval		: 1000
<output truncated=""></output>		
Vlan 951:		
MLD snooping		: Disabled
MLDv1 immediate leave		: Disabled
Explicit host tracking		: Enabled
Multicast router learning mode	Э	: pim-dvmrp
Robustness variable		: 3
Last listener query count		: 2
Last listener query interval		: 1000

Related Commands	Command	Description
	ipv6 mld snooping	Enables IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping globally or on the specified VLAN.

show ipv6 mld snooping mrouter

To display dynamically learned and manually configured IP version 6 (IPv6) Multicast Listener Discovery (MLD) switch ports for the switch or a VLAN, use the **show ipv6 mld snooping mrouter** command.

show ipv6 mld snooping mrouter [vlan vlan-id]

Syntax Description	vlan vlan-id	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.		
Command Modes	User EXEC mode			
Command History	Release	Modification		
	12.2(40)SG	This command was introduced on Catalyst 4500.		
Usage Guidelines	Use this command	to display MLD snooping switch ports for the switch or for a specific VLAN.		
	VLAN numbers 10 in MLD snooping.	02 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used		
Examples	characteristics for a	of output from the show ipv6 mld snooping mrouter command. It displays snooping all VLANs on the switch that are participating in MLD snooping.		
	Vlan ports	i mld snooping mrouter		
	2 Gi1/0/11(72 Gi1/0/11(200 Gi1/0/11)	(dynamic)		
	This is an example of output from the show ipv6 mld snooping mrouter vlan command. It shows multicast switch ports for a specific VLAN.			
	Vlan ports	mld snooping mrouter vlan 100		
	2 Gi1/0/11(dynamic)		
Related Commands	Command	Description		
	ipv6 mld snooping	g Enables IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping globally or on the specified VLAN.		

interface.

ipv6 mld snooping vlan

Configures IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping parameters on the VLAN

show ipv6 mld snooping querier

To display IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping querier-related information most recently received by the switch or the VLAN, use the **show ipv6 mld snooping querier** command.

show ipv6 mld snooping querier [vlan vlan-id]

Syntax Description	vlan vlan-id	(Optional) Specify a	VLAN; the range is 1 to 1001 and 1006 to 4094.		
Command Modes	User EXEC mode				
Command History	Release	Modification			
	12.2(40)SG	This command was ir	introduced on the Catalyst 4500.		
Usage Guidelines	Use the show ipv6 mld snooping querier command to display the MLD version and IPv6 address of a detected device that sends MLD query messages, which is also called a <i>querier</i> . A subnet can have multiple multicast switches but has only one MLD querier. The querier can be a Layer 3 switch.				
	The show ipv6 mld snooping querier command output also shows the VLAN and interface on which the querier was detected. If the querier is the switch, the output shows the <i>Port</i> field as <i>Router</i> . If the querier is a router, the output shows the port number on which the querier is learned in the <i>Port</i> field.				
	The output of the show ipv6 mld snoop querier vlan command displays the information received in response to a query message from an external or internal querier. It does not display user-configured VLAN values, such as the snooping robustness variable on the particular VLAN. This querier information is used only on the MASQ message that is sent by the switch. It does not override the user-configured robustness variable that is used for aging out a member that does not respond to query messages.				
	VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.				
Examples	This is an example	of output from the show ipv	v6 mld snooping querier command:		
	Switch> show ipv6 Vlan IP Addr	mld snooping querier ess MLD Ver	ersion Port		
	2 FE80::2	01:C9FF:FE40:6000 v1	Gi3/0/1		
	This is an example of output from the show ipv6 mld snooping querier vlan command:				
		<pre>mld snooping querier vla ::201:C9FF:FE40:6000 : 1000s</pre>	.an 2		

Related Commands	Command	Description	
	ipv6 mld snooping	Enables IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping globally or on the specified VLAN.	
	ipv6 mld snooping last-listener-query-count	Configures IP version 6 (IPv6) Multicast Listener Discovery Mulitcast Address Specific Queries (MASQs) that will be sent before aging out a client. Configures IP version 6 (IPv6) MLD snooping last-listener query interval on the switch or on a VLAN.	
	ipv6 mld snooping last-listener-query-interval		
	ipv6 mld snooping robustness-variable	Configures the number of IP version 6 (IPv6) MLD queries that the switch sends before deleting a listener that does not respond.	
	ipv6 mld snooping tcn	Configures IP version 6 (IPv6) MLD Topology Change Notifications (TCNs).	

show issu capability

To display the ISSU capability for a client, use the **show issu capability** command.

show issu capability {entries | groups | types } [client_id]

P 4 D	-					
Syntax Description	entries	Displays a list of Capability Types and Dependent Capability Types that a included in a single Capability Entry. Types within an entry can also be independent.				
	groups	Displays a list of Capability Entries in priority order (the order that they will be negotiated on a session).				
	types	Displays an ID that identifies a particular capability.				
	client_id	(Optional) Identifies the client registered to the ISSU infrastructure.				
		To obtain a list of client IDs, use the show issu clients command.				
Defaults	This command has	no default settings.				
Command Modes	User EXEC					
Command History	Release	Modification				
	12.2(31)SGA	This command was introduced on the Catalyst 4500 series switch.				
Usage Guidelines	Capability is a functionality that an ISSU client can support and is required to interoperate with peers.					
		re client establishes its session with the peer, an ISSU negotiation takes place. The uses the registered information to negotiate the capabilities and the message version e session.				
Examples	The following exam (clientid=2082):	ple shows how to display the ISSU capability types for the IP host ISSU client				
Examples	(clientid=2082):	aple shows how to display the ISSU capability types for the IP host ISSU client capability types 2082 Entity_ID = 1 :				
Examples	<pre>(clientid=2082): Switch#show issu (Client_ID = 2082, Cap_Type = 0 Switch#</pre>	capability types 2082				

The following example shows how to display the ISSU capabilities groups for the IP host ISSU client (clientid=2082):

```
Switch#show issu capability groups 2082
Client_ID = 2082, Entity_ID = 1 :
    Cap_Group = 1 :
    Cap_Entry = 1
    Cap_Type = 0
```

Switch#

Related Commands	Command	Description	
	show issu clients	Displays the ISSU clients.	

show issu clients

To display the ISSU clients, use the show issu clients command.

show issu clients [peer_uid]

Syntax Description	peer_uid	(Optional) Displays a list of clients registered to ISSU infrastructure at the peer supervisor engine.			
Defaults	Displays a list of clie command is entered.	nts registered to the ISSU infrastructure at the supervisor engine where the			
Command Modes	User EXEC				
Command History	Release	Modification			
oommunu motory	12.2(31)SGA	This command was introduced on the Catalyst 4500 series switch.			
		·			
Usage Guidelines	-	ersioning functionality, a client must first register itself, client capability, and client with the ISSU infrastructure during the system initialization.			
Examples	The following examp	le shows how to display the ISSU clients:			
	Switch# show issu clients Client_ID = 2, Client_Name = ISSU Proto client, Entity_Count = 1				
		ient_Name = ISSU RF, Entity_Count = 1			
		<pre>ient_Name = ISSU CF client, Entity_Count = 1</pre>			
		<pre>ient_Name = ISSU Network RF client, Entity_Count = 1 .ient_Name = ISSU CONFIG SYNC, Entity_Count = 1</pre>			
		ient_Name = ISSU ifIndex sync, Entity_Count = 1			
	Client_ID = 9, Cl	ient_Name = ISSU IPC client, Entity_Count = 1			
		lient_Name = ISSU IPC Server client, Entity_Count = 1			
		lient_Name = ISSU Red Mode Client, Entity_Count = 1 Client_Name = ISSU rfs client, Entity_Count = 1			
		Client_Name = ISSU ifs client, Entity_Count = 1			
		Client_Name = ISSU Event Manager client, Entity_Count = 1			
	_	Client_Name = CEF Push ISSU client, Entity_Count = 1			
		Client_Name = ISSU XDR client, Entity_Count = 1 Client_Name = ISSU SNMP client, Entity_Count = 1			
	$Client_ID = 2010,$	Client_Name = ARP HA, Entity_Count = 1			
	$Client_{ID} = 2012,$	Client_Name = ISSU HSRP Client, Entity_Count = 1			
	$Client_{ID} = 2021,$	Client_Name = XDR Int Priority ISSU client, Entity_Count = 1			
	Client_ID = 2022, Client_ID = 2023,	Client_Name = XDR Proc Priority ISSU client, Entity_Count = 1 Client_Name = FIB HWIDB ISSU client, Entity_Count = 1			
	Client_ID = 2024,	Client_Name = FIB IDB ISSU client, Entity_Count = 1			
	$Client_{ID} = 2025,$	Client_Name = FIB HW subblock ISSU client, Entity_Count = 1			
	$Client_{ID} = 2026,$	Client_Name = FIB SW subblock ISSU client, Entity_Count = 1			
	Client_ID = 2027 ,	Client_Name = Adjacency ISSU client, Entity_Count = 1 Client_Name = FIB IPV4 ISSU client, Entity_Count = 1			
	$crrenc_{ID} = 2028,$	CITENCTNAME = LID ILAA ISOO CITENC' RUCICATORNI = I			

Client_ID = 2054, Client_Name = ISSU process client, Entity_Count = 1 Client_ID = 2058, Client_Name = ISIS ISSU RTR client, Entity_Count = 1 Client_ID = 2059, Client_Name = ISIS ISSU UPD client, Entity_Count = 1 Client_ID = 2067, Client_Name = ISSU PM Client, Entity_Count = 1 Client_ID = 2068, Client_Name = ISSU PAGP_SWITCH Client, Entity_Count = 1 Client_ID = 2070, Client_Name = ISSU Port Security client, Entity_Count = 1 Client_ID = 2071, Client_Name = ISSU Switch VLAN client, Entity_Count = 1 Client_ID = 2072, Client_Name = ISSU dot1x client, Entity_Count = 1 Client_ID = 2073, Client_Name = ISSU STP, Entity_Count = 1 Client_ID = 2077, Client_Name = ISSU STP MSTP, Entity_Count = 1 Client_ID = 2078, Client_Name = ISSU STP IEEE, Entity_Count = 1 Client_ID = 2079, Client_Name = ISSU STP RSTP, Entity_Count = 1 Client_ID = 2081, Client_Name = ISSU DHCP Snooping client, Entity_Count = 1 Client_ID = 2082, Client_Name = ISSU IP Host client, Entity_Count = 1 Client_ID = 2083, Client_Name = ISSU Inline Power client, Entity_Count = 1 Client_ID = 2084, Client_Name = ISSU IGMP Snooping client, Entity_Count = 1 Client_ID = 4001, Client_Name = ISSU C4K Chassis client, Entity_Count = 1 Client_ID = 4002, Client_Name = ISSU C4K Port client, Entity_Count = 1 Client_ID = 4003, Client_Name = ISSU C4K Rkios client, Entity_Count = 1 Client_ID = 4004, Client_Name = ISSU C4K HostMan client, Entity_Count = 1 Client_ID = 4005, Client_Name = ISSU C4k GaliosRedundancy client, Entity_Count = 1 Base Clients: Client_Name = ISSU Proto client Client_Name = ISSU RF Client_Name = ISSU CF client Client Name = ISSU Network RF client Client_Name = ISSU CONFIG SYNC Client_Name = ISSU ifIndex sync Client_Name = ISSU IPC client Client_Name = ISSU IPC Server client Client Name = ISSU Red Mode Client Client_Name = ISSU rfs client Client_Name = ISSU ifs client Client_Name = ISSU Event Manager client Client_Name = CEF Push ISSU client Client_Name = ISSU XDR client Client_Name = ARP HA Client_Name = XDR Int Priority ISSU client Client_Name = XDR Proc Priority ISSU client Client Name = FIB HWIDB ISSU client Client_Name = FIB IDB ISSU client Client_Name = FIB HW subblock ISSU client Client_Name = FIB SW subblock ISSU client Client_Name = Adjacency ISSU client Client_Name = FIB IPV4 ISSU client Client_Name = ISSU process client Client_Name = ISSU PM Client Client_Name = ISSU C4K Chassis client Client_Name = ISSU C4K Port client Client_Name = ISSU C4K Rkios client Client_Name = ISSU C4K HostMan client Client_Name = ISSU C4k GaliosRedundancy client

Related Commands	Command	Description		
	show issu capability	Displays the ISSU capability for a client.		
	show issu entities	Displays the ISSU entity information.		

show issu comp-matrix

To display information regarding the In Service Software Upgrade (ISSU) compatibility matrix, use the **show issu comp-matrix** command.

show issu comp-matrix {negotiated | stored | xml}

Syntax Description	negotiated	Displays negotiated compatibility matrix information.				
	stored	Displays stored compatibility matrix information.				
	xml	Displays negotiated compatibility matrix information in XML format.				
Defaults	This command has n	o default settings.				
Command Modes	User EXEC					
Command History	Release	Modification				
	12.2(31)SGA	This command was introduced on the Catalyst 4500 series switch.				
Usage Guidelines	Before attempting an ISSU, you should know the compatibility level between the old and the new Cisco IOS software versions on the active and the standby-supervisor engines. ISSU will not work if the two versions are incompatible. The compatibility matrix is available on Cisco.com so that you can also veiw in advance whether an upgrade can be performed with the ISSU process. The compatibility matrix during the ISSU process and					
	later by entering the show issu comp-matrix command. To display information on the negotiation of the compatibility matrix data between two software versions on a given system, use the show issu comp-matrix negotiated command.					
	Compatibility matrix data is stored with each Cisco IOS software image that supports ISSU capability. To display stored compatibility matrix information, use the show issu comp-matrix stored command.					
	The compatibility matrix information are built-in any IOS ISSU image. The ISSU infrastructure performs a matrix lookup as soon as the communication with the standby supervisor engine is established. There are three possible results from the lookup operation:					
	• Compatible—The Base-level system infrastructure and all optional HA-aware subsystems are compatible. In-service upgrade or downgrade between these versions will succeed with minimal service impact.					
	Although an in-s subsystems will	patible—One or more of the optional HA-aware subsystems are not compatible. service upgrade or downgrade between these versions will succeed, some not be able to maintain their state during the switchover. Prior to attempting an de or downgrade, the impact of this on operation and service of the switch must be fully.				

• Incompatible—A set of core system infrastructure must be able to execute in a stateful manner for SSO to function correctly. If any of these "required" features or subsystems is not compatible in two different IOS images, the two versions of the Cisco IOS images are declared "Incompatible". This means that an in-service upgrade or downgrade between these versions is not possible. The systems operates in RPR mode during the period when the versions of IOS at the active and standby supervisor engines differ.

Examples

This example displays negotiated compatibility matrix information:

Switch# show issu comp-matrix negotiated

CardType: WS-C4507R(112), Uid: 2, Image Ver: 12.2(31)SGA Image Name: cat4500-ENTSERVICES-M

2 1 262151 3 1 COMPATI 3 1 262160 5 1 COMPATI 4 1 262163 9 1 COMPATI	BLE BLE BLE
4 1 262163 9 1 COMPATI	BLE
5 1 262186 25 1 COMPATI	BLE
7 1 262156 10 1 COMPATE	BLE
8 1 262148 7 1 COMPATI	BLE
9 1 262155 1 1 COMPATE	BLE
10 1 262158 2 1 COMPATE	BLE
11 1 262172 6 1 COMPATI	BLE
100 1 262166 13 1 COMPATE	BLE
110 113 262159 14 1 COMPATE	BLE
200 1 262167 24 1 COMPATE	BLE
2002 1 UNAVAIL	ABLE
2003 1 262185 23 1 COMPATE	BLE
2004 1 262175 16 1 COMPATE	BLE
2008 1 262147 26 1 COMPATE	BLE
2008 1 262168 27 1 COMPATE	BLE
2010 1 262171 32 1 COMPATE	BLE
2012 1 262180 31 1 COMPATE	BLE
2021 1 262170 41 1 COMPATE	BLE
2022 1 262152 42 1 COMPATE	BLE
2023 1 UNAVAIL	ABLE
2024 1 UNAVAIL	ABLE
2025 1 UNAVAIL	ABLE
2026 1 UNAVAIL	ABLE
2027 1 UNAVAIL	ABLE
2028 1 UNAVAIL	ABLE
2054 1 262169 8 1 COMPATE	BLE
2058 1 262154 29 1 COMPATE	BLE
2059 1 262179 30 1 COMPATE	BLE
2067 1 262153 12 1 COMPATE	BLE
2068 1 196638 40 1 COMPATE	BLE
2070 1 262145 21 1 COMPATI	BLE
2071 1 262178 11 1 COMPATE	BLE
2072 1 262162 28 1 COMPATE	BLE
2073 1 262177 33 1 COMPATE	BLE
2077 1 262165 35 1 COMPATE	BLE
2078 1 196637 34 1 COMPATE	BLE
2079 1 262176 36 1 COMPATI	BLE
2081 1 262150 37 1 COMPATE	BLE
2082 1 262161 39 1 COMPATE	BLE
2083 1 262184 20 1 COMPATI	BLE
2084 1 262183 38 1 COMPATI	BLE
4001 101 262181 17 1 COMPATI	BLE
4002 201 262164 18 1 COMPATI	BLE

4003 4004 4005	301 401 1	262182 262146 262149	19 1 22 1 4 1		COMPATI COMPATI COMPATI	IBLE
Message Cid	group Eid	summary: GrpId	Sid	pSid	pUid	Nego Result
=======	=======	===========	==========	========		===========
2	1	1	262151	3	1	Y
3	1	1	262160	5	1	Y
4	1	1	262163	9	1	Y
5	1	1	262186	25	1	Y
7 8	1 1	1 1	262156	10 7	1 1	Y
o 9	1	1	262148 262155	1	1	Y Y
10	1	1	262155	2	1	Y
11	1	1	262172	6	1	Ŷ
100	1	1	262166	13	1	Y
110	113	115	262159	14	1	Y
200	1	1	262167	24	1	Y
2002	1	2	-	-	-	N - did not negotiate
2003	1	1	262185	23	1	Y
2004	1	1	262175	16	1	Y
2008 2008	1 1	1 2	262147 262168	26 27	1 1	Y Y
2008	1	1	262108	32	1	Y Y
2010	1	1	262180	31	1	Y
2021	1	1	262170	41	1	Ŷ
2022	1	1	262152	42	1	Y
2023	1	1	-	-	-	N - did not negotiate
2024	1	1	-	-	-	N - did not negotiate
2025	1	1	-	-	-	N - did not negotiate
2026	1	1	-	-	-	N - did not negotiate
2027	1	1	-	-	-	N - did not negotiate
2028	1	1	-	-	_	N - did not negotiate
2054 2058	1 1	1 1	262169 262154	8 29	1 1	Y Y
2058	1	1	262154	30	1	Y Y
2055	1	1	262153	12	1	Y
2068	1	1	196638	40	1	Ŷ
2070	1	1	262145	21	1	Y
2071	1	1	262178	11	1	Y
2072	1	1	262162	28	1	Y
2073	1	1	262177	33	1	Y
2077	1	1	262165	35	1	Y
2078	1	1	196637	34	1	Y
2079	1	1	262176	36	1	Y
2081 2082	1 1	1 1	262150 262161	37 39	1 1	Y Y
2082	1	1	262184	20	1	I Y
2084	1	1	262183	38	1	Y
4001	101	1	262181	17	1	Ŷ
4002	201	1	262164	18	1	Y
4003	301	1	262182	19	1	Y
4004	401	1	262146	22	1	Y
4005	1	1	262149	4	1	Y
List of				Dage /I	Iom Dogo	
Cid ========		ent Name ========			Non-Base	
2		J Proto cl		Base		
3		JRF		Base		
4	ISSU	J CF clien	.t	Base		
5		J Network		Base		
7	ISSU	J CONFIG S	YNC	Base		

8	ISSU ifIndex sync	Base
9	ISSU IPC client	Base
10	ISSU IPC Server client	Base
11	ISSU Red Mode Client	Base
100	ISSU rfs client	Base
110	ISSU ifs client	Base
200	ISSU Event Manager clien	tBase
2002	CEF Push ISSU client	Base
2003	ISSU XDR client	Base
2004	ISSU SNMP client	Non-Base
2008	ISSU Tableid Client	Base
2010	ARP HA	Base
2012	ISSU HSRP Client	Non-Base
2021	XDR Int Priority ISSU cl	iBase
2022	XDR Proc Priority ISSU c	lBase
2023	FIB HWIDB ISSU client	Base
2024	FIB IDB ISSU client	Base
2025	FIB HW subblock ISSU cli	eBase
2026	FIB SW subblock ISSU cli	eBase
2027	Adjacency ISSU client	Base
2028	FIB IPV4 ISSU client	Base
2054	ISSU process client	Base
2058	ISIS ISSU RTR client	Non-Base
2059	ISIS ISSU UPD client	Non-Base
2067	ISSU PM Client	Base
2068	ISSU PAGP_SWITCH Client	Non-Base
2070	ISSU Port Security clien	tNon-Base
2071	ISSU Switch VLAN client	Non-Base
2072	ISSU dot1x client	Non-Base
2073	ISSU STP	Non-Base
2077	ISSU STP MSTP	Non-Base
2078	ISSU STP IEEE	Non-Base
2079	ISSU STP RSTP	Non-Base
2081	ISSU DHCP Snooping clien	tNon-Base
2082	ISSU IP Host client	Non-Base
2083	ISSU Inline Power client	Non-Base
2084	ISSU IGMP Snooping clien	tNon-Base
4001	ISSU C4K Chassis client	Base
4002	ISSU C4K Port client	Base
4003	ISSU C4K Rkios client	Base
4004	ISSU C4K HostMan client	Base
4005	ISSU C4k GaliosRedundanc	

This example displays stored compatibility matrix information:

Switch> show issu comp-matrix stored

Number of Matrices in Table = 1
Related Commands	Command	Description
	show issu clients	Displays the ISSU clients.
	show issu sessions	Displays ISSU session information for a specified client.

show issu endpoints

To display the ISSU endpoint information, use the show issu endpoints command.

	show issu endpoi	nts			
Syntax Description	This command has no	arguments or k	eywords		
Defaults	This command has no	default settings			
Command Modes	User EXEC				
Command History	Release	Modificatio	n		
	12.2(31)SGA	This comm	and was introdu	ced on the C	Catalyst 4500 series switch.
	perform session negot	iation for ISSU	clients.		
Examples	The following exampl	e shows how to	display the ISS	U endpoints	:
	Switch# show issu en	=	nt = 46		
	$My_Unique_ID = 1/0x$	1, 0110110_000	10		
	This endpoint comm	unicates with	1 peer endpoin		
		unicates with	1 peer endpoin ER XFORM	ts : ERP 1	Compatibility Same

Related Commands	Command	Description
	show issu clients	Displays the ISSU clients.

show issu entities

To display the ISSU entity information, use the show issu entities command.

show issu entities [client_id]

Syntax Description	client_id	(Optional) ISSU client ID.
Defaults	This command has	no default settings.
Command Modes	User EXEC	
Command History	Release	Modification
	12.2(31)SGA	This command was introduced on the Catalyst 4500 series switch.
Usage Guidelines		roup of sessions with some common attributes (like capability list and message type). SU clients on the Catalyst 4500 series switch have only one entity.
Examples	The following exam	pple shows how to display the entity information for a specified ISSU client:
	_	
Related Commands	Command	Description
	show issu clients	Displays the ISSU clients.

show issu fsm

Note	This command is not	t intended for end-	users.	
	To display the ISSU show issu fsm comn		ue (FSM) informat	ion corresponding to an ISSU session, use the
	show issu fsm [.	session_id]		
Syntax Description	session_id	(Optional) P session.	rovides detailed in	nformation about the FSM for the specified
Defaults	This command has n	o default settings.		
Command Modes	User EXEC			
Command History	Release	Modification	1	
	12.2(31)SGA	This comma	nd was introduced	l on the Catalyst 4500 series switch.
Examples	The following exam	ple displays and ve		ate after LOADVERSION:
Examples	Switch# show issu			ate after LOADVERSION:
Examples	Switch# show issu Session_ID = 26 :	fsm 26	erifies the ISSU st	
Examples	Switch# show issu Session_ID = 26 : FSM_Name	fsm 26 Curr_State	erifies the ISSU st	Error_Reason
Examples	Switch# show issu Session_ID = 26 : FSM_Name FSM_L1	fsm 26 Curr_State TRANS	old_State A_VER	Error_Reason none
Examples	Switch# show issu Session_ID = 26 : FSM_Name FSM_L1 FSM_L2_HELLO	fsm 26 Curr_State TRANS EXIT	Old_State A_VER RCVD	Error_Reason none none
Examples	Switch# show issu Session_ID = 26 : FSM_Name FSM_L1 FSM_L2_HELLO FSM_L2_A_CAP	fsm 26 Curr_State TRANS EXIT A_EXIT	old_State A_VER	Error_Reason none
Examples	Switch# show issu Session_ID = 26 : FSM_Name FSM_L1 FSM_L2_HELLO	fsm 26 Curr_State TRANS EXIT	Old_State A_VER RCVD A_RSP	Error_Reason none none none
Examples	Switch# show issu Session_ID = 26 : FSM_Name FSM_L1 FSM_L2_HELLO FSM_L2_A_CAP FSM_L2_P_CAP	fsm 26 Curr_State TRANS EXIT A_EXIT P_INIT	Old_State A_VER RCVD A_RSP unknown	Error_Reason none none none none
Examples	Switch# show issu Session_ID = 26 : FSM_Name FSM_L1 FSM_L2_HELLO FSM_L2_A_CAP FSM_L2_A_CAP FSM_L2_P_CAP FSM_L2_A_VER FSM_L2_P_VER FSM_L2_TRANS	fsm 26 Curr_State TRANS EXIT A_EXIT P_INIT A_EXIT P_INIT COMP	Old_State A_VER RCVD A_RSP unknown A_RES_RSP	Error_Reason none none none none none
Examples	Switch# show issu Session_ID = 26 : FSM_Name FSM_L1 FSM_L2_HELLO FSM_L2_A_CAP FSM_L2_P_CAP FSM_L2_A_VER FSM_L2_P_VER FSM_L2_TRANS Current FSM is FS	fsm 26 Curr_State TRANS EXIT A_EXIT P_INIT A_EXIT P_INIT COMP M_L2_TRANS	Old_State A_VER RCVD A_RSP unknown A_RES_RSP unknown	Error_Reason none none none none none none
Examples	Switch# show issu Session_ID = 26 : FSM_Name FSM_L1 FSM_L2_HELLO FSM_L2_A_CAP FSM_L2_A_CAP FSM_L2_P_CAP FSM_L2_A_VER FSM_L2_P_VER FSM_L2_TRANS	fsm 26 Curr_State TRANS EXIT A_EXIT P_INIT A_EXIT P_INIT COMP M_L2_TRANS ible	Old_State A_VER RCVD A_RSP unknown A_RES_RSP unknown COMP	Error_Reason none none none none none none none
Examples Related Commands	Switch# show issu Session_ID = 26 : FSM_Name FSM_L1 FSM_L2_HELLO FSM_L2_A_CAP FSM_L2_A_CAP FSM_L2_P_CAP FSM_L2_A_VER FSM_L2_P_VER FSM_L2_TRANS Current FSM is FS Session is compat Negotiation start	fsm 26 Curr_State TRANS EXIT A_EXIT P_INIT A_EXIT P_INIT COMP M_L2_TRANS ible	Old_State A_VER RCVD A_RSP unknown A_RES_RSP unknown COMP	Error_Reason none none none none none none none
	<pre>Switch# show issu Session_ID = 26 : FSM_Name FSM_L1 FSM_L2_HELLO FSM_L2_A_CAP FSM_L2_A_CAP FSM_L2_A_VER FSM_L2_A_VER FSM_L2_TRANS Current FSM is FS Session is compat Negotiation start Switch#</pre>	fsm 26 Curr_State TRANS EXIT A_EXIT P_INIT A_EXIT P_INIT COMP M_L2_TRANS ible	Old_State A_VER RCVD A_RSP unknown A_RES_RSP unknown COMP	Error_Reason none none none none none none 0.148 seconds

show issu message

To display checkpoint messages for a specified ISSU client, use the show issu message command.

show issu message {groups | types} [client_id]

Syntax Description	groups	Displays information on Message Group supported by the specified client.
	types	Displays information on all Message Types supported by the specified client.
	client_id	(Optional) Specifies a client ID.
Defaults		specified, displays message groups or message types information for all clients ISSU infrastructure.
Command Modes	User EXEC	
Command History	Release	Modification
-	12.2(31)SGA	This command was introduced on the Catalyst 4500 series switch.
Examples	to be used during	ample shows how to display the message groups for Client_id 2082:
		u message groups 2082
		2, Entity_ID = 1 : up = 1 : Message_Type = 1, Version_Range = 1 ~ 2
	Switch#	Message_Type = 2, Version_Range = 1 ~ 2
	The following ex	ample shows how to display the message types for Client_id 2082:
	Switch# show iss	

Related Commands	Command	Description
	show issu clients	Displays the ISSU clients.

show issu negotiated

To display the negotiated capability and message version information of the ISSU clients, use the **show issu negotiated** command.

show issu negotiated {capability | version} [session_id]

Syntax Description	capability	Displays all negotiated capabilities.
	version	Displays details of all negotiated messages.
	session_id	(Optional) Specifies the ISSU session ID for which the capability or version information is displayed.
Defaults	Displays negotiated ca	pability or version information for all ISSU sessions.
Command Modes	User EXEC	
Command History	Release	Modification
	12.2(31)SGA	This command was introduced on the Catalyst 4500 series switch.
Examples	The following example	shows how to display the message types for a specific group:
	Switch# show issu ne Session_ID = 26 : Cap_Type = 0,	gotiated capability 26 Cap_Result = 1 No cap value assigned
	Switch# show issu ne Session_ID = 26 :	<pre>gotiated version 26 1, Negotiated_Version = 1, Message_MTU = 44</pre>
Related Commands	Command	Description
	show issu sessions	Displays ISSU session information for a specified client.

show issu rollback-timer

To display ISSU rollback-timer status, use the show issu rollback-timer command.

show issu rollback-timer

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

- **Defaults** This command has no default settings.
- **Command Modes** Priviledged EXEC

 Release
 Modification

 12.2(31)SGA
 This command was introduced on the Catalyst 4500 series switch.

Examples The following example shows how to display the rollback-timer status:

Switch**#show issu rollback-timer** Rollback Process State = Not in progress Configured Rollback Time = 45:00

Switch#

Related Commands	Command	Description
	issu acceptversion	Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically stopped during the ISSU process.
	issu runversion	Forces a change from the active supervisor engine to the standby supervisor engine and causes the newly active supervisor engine to run the new image specified in the issu loadversion command.

show issu sessions

To display ISSU session information for a specified client, use the **show issu sessions** command.

show issu sessions [client_id]

Syntax Description	client_id	(Optional) Specifies the ISSU client ID.
Defaults	Displays session inf	formation for all clients registered to the ISSU infrastructure.
Command Modes	User EXEC	
Command History	Release	Modification
	12.2(31)SGA	This command was introduced on the Catalyst 4500 series switch.
Usage Guidelines	negotiation message	onal and a reliable connection is established between two endpoints. Sync-data and as are sent to the peer endpoint through a session. On a Catalyst 4500 series switch, ient has a maximum of one session at each endpoint.
		re client establishes its session with the peer, an ISSU negotiation takes place. The uses the registered information to negotiate the capabilities and the message version e session.
Examples	The following exam	ple shows how to display the rollback-timer status:
	Switch# show issu : Client_ID = 2072,	
	*** Session_ID =	26, Session_Name = dot1x :
	Peer Peer M UniqueID Sid 2 26	Negotiate Negotiated Cap Msg Session Role Result GroupID GroupID Signature PRIMARY COMPATIBLE 1 1 0 (no policy)
	Nego_Sess Nego_Sess	ession Info for This Message Session: sion_ID = 26 sion_Name = dot1x t_Mtu = 17884
Related Commands	Command	Description
	show issu clients	Displays the ISSU clients.

show issu state

To display the ISSU state and current booted image name during the ISSU process, use the **show issu state** command.

show issu state [slot_number] [detail]

Syntax Description	slot_number	(Optional) Specifies the slot number whose ISSU state needs to be displayed (1 or 2).
	detail	(Optional) Provides detailed information about the state of the active and standby supervisor engines.
Defaults	The command displ supervisor engines.	ays the ISSU state and current booted image name of both the active and standby
Command Modes	Privileged EXEC m	ode
Command History	Release	Modification
-	12.2(31)SGA	This command was introduced on the Catalyst 4500 series switch.
		y supervisor engine and the standby supervisor engine to transition to SSO mode. If issu state command too soon, you might not see the information you need.
Fxamples	you enter the show	issu state command too soon, you might not see the information you need.
Examples	you enter the show The following exam	issu state command too soon, you might not see the information you need. ple displays and verifies the ISSU state after LOADVERSION:
Examples	you enter the show	issu state command too soon, you might not see the information you need. ple displays and verifies the ISSU state after LOADVERSION:
Examples	you enter the show The following exam	<pre>issu state command too soon, you might not see the information you need. ple displays and verifies the ISSU state after LOADVERSION: state detail Slot = 1 RP State = Active</pre>
Examples	you enter the show The following exam Switch# show issu	<pre>issu state command too soon, you might not see the information you need. ple displays and verifies the ISSU state after LOADVERSION: state detail Slot = 1 RP State = Active ISSU State = Load Version</pre>
Examples	you enter the show i The following exam Switch# show issu	<pre>issu state command too soon, you might not see the information you need. ple displays and verifies the ISSU state after LOADVERSION: state detail Slot = 1 RP State = Active</pre>
Examples	you enter the show The following exam Switch# show issu Or Pr:	<pre>issu state command too soon, you might not see the information you need. ple displays and verifies the ISSU state after LOADVERSION: state detail Slot = 1 RP State = Active ISSU State = Load Version Boot Variable = bootflash:old_image,12 perating Mode = Stateful Switchover imary Version = bootflash:old_image</pre>
Examples	you enter the show The following exam Switch# show issu Or Pr: Secon	<pre>issu state command too soon, you might not see the information you need. ple displays and verifies the ISSU state after LOADVERSION: state detail Slot = 1 RP State = Active ISSU State = Load Version Boot Variable = bootflash:old_image,12 perating Mode = Stateful Switchover</pre>
Examples	you enter the show The following exam Switch# show issu Or Pr: Secon	<pre>issu state command too soon, you might not see the information you need. ple displays and verifies the ISSU state after LOADVERSION: state detail Slot = 1 RP State = Active ISSU State = Load Version Boot Variable = bootflash:old_image,12 perating Mode = Stateful Switchover imary Version = bootflash:old_image ndary Version = bootflash:new_image</pre>
Examples	you enter the show The following exam Switch# show issu Or Pr: Secon	<pre>issu state command too soon, you might not see the information you need. ple displays and verifies the ISSU state after LOADVERSION: state detail Slot = 1 RP State = Active ISSU State = Load Version Boot Variable = bootflash:old_image,12 perating Mode = Stateful Switchover imary Version = bootflash:old_image ndary Version = bootflash:old_image rrent Version = bootflash:old_image Slot = 2 RP State = Standby</pre>
Examples	you enter the show The following exam Switch# show issu I Or Pr: Secor Cur	<pre>issu state command too soon, you might not see the information you need. ple displays and verifies the ISSU state after LOADVERSION: state detail Slot = 1 RP State = Active ISSU State = Load Version Boot Variable = bootflash:old_image,12 perating Mode = Stateful Switchover imary Version = bootflash:old_image ndary Version = bootflash:old_image rrent Version = bootflash:old_image Slot = 2 RP State = Standby ISSU State = Load Version</pre>
Examples	you enter the show in The following exam Switch# show issu I Or Pr: Secon Cun	<pre>issu state command too soon, you might not see the information you need. ple displays and verifies the ISSU state after LOADVERSION: state detail Slot = 1 RP State = Active ISSU State = Load Version Boot Variable = bootflash:old_image,12 perating Mode = Stateful Switchover imary Version = bootflash:old_image ndary Version = bootflash:old_image rrent Version = bootflash:old_image Slot = 2 RP State = Standby</pre>
Examples	you enter the show in The following exam Switch# show issu I Or Pr: Secon Cun I Or Pr: Secon Cun	<pre>issu state command too soon, you might not see the information you need. ple displays and verifies the ISSU state after LOADVERSION: state detail Slot = 1 RP State = Active ISSU State = Load Version Boot Variable = bootflash:old_image,12 perating Mode = Stateful Switchover imary Version = bootflash:old_image rrent Version = bootflash:old_image Slot = 2 RP State = Standby ISSU State = Load Version Boot Variable = bootflash:new_image,12;bootflash:old_image,12 perating Mode = Stateful Switchover </pre>
Examples	you enter the show in The following exam Switch# show issu I Or Pr: Secon Cun I Or Pr: Secon Cun Secon Cun	<pre>issu state command too soon, you might not see the information you need. ple displays and verifies the ISSU state after LOADVERSION: state detail Slot = 1 RP State = Active ISSU State = Load Version Boot Variable = bootflash:old_image,12 perating Mode = Stateful Switchover imary Version = bootflash:old_image ndary Version = bootflash:old_image rrent Version = bootflash:old_image Slot = 2 RP State = Standby ISSU State = Load Version Boot Variable = bootflash:new_image,12;bootflash:old_image,12;bootflash:0ld_image,12;bo</pre>

Related Commands	Command	Description
	issu abortversion	Cancels the ISSU upgrade or the downgrade process in progress and restores the switch to its state before the start of the process.
	issu acceptversion	Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically stopped during the ISSU process.
	issu commitversion	Loads the new Cisco IOS software image into the new standby supervisor engine.
	issu loadversion	Starts the ISSU process.
	issu runversion	Forces a change from the active supervisor engine to the standby supervisor engine and causes the newly active supervisor engine to run the new image specified.

show I2protocol-tunnel

To display information about the Layer 2 protocol tunnel ports, use the **show l2protocol-tunnel** command. This command displays information for the interfaces with protocol tunneling enabled.

show l2protocol-tunnel [interface interface-id] [[summary] | {begin | exclude | include}
expression]

Syntax Description	interface interface-id	(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 the lines that match the specified <i>expression</i> .
	expression	(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.
	12.2(25)EW	Added support for the 10-Gigabit Ethernet interface.

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.

Examples

This is an example of output from the **show l2protocol-tunnel** command:

Switch> show 12protocol-tunnel

COS for Encapsulated Packets: 5

Port	Protocol	Shutdown	Drop	Encapsulation	Decapsulation	Drop
		Threshold	Threshold	Counter	Counter	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
	udld		900	0	0	0
Fa0/12	cdp			2356	0	0
	stp			11787	0	0
	vtp			81	0	0
	pagp			0	0	0
	lacp			849	0	0
	udld			0	0	0
Fa0/13	cdp			2356	0	0
	stp			11788	0	0
	vtp			81	0	0
	pagp			0	0	0
	lacp			849	0	0
	udld			0	0	0
a						

Switch#

This is an example of output from the show l2protocol-tunnel summary command:

Switch> show 12protocol-tunnel summary COS for Encapsulated Packets: 5

Port	Protocol	Threshold (cdp/stp/vtp)	Drop Threshold (cdp/stp/vtp) (pagp/lacp/udld)	Status
Fa0/10	stp vtp	//	//	up
pa	gp lacp udld	//	//	
Fa0/11	cdp stp vtp	1100/1100/1100	//	up
pa	gp lacp udld	//	900/ 900/ 900	
Fa0/12	cdp stp vtp	//	//	up
pa	gp lacp udld	//	//	
Fa0/13	cdp stp vtp	//	//	up
pa	gp lacp udld	//	//	
Fa0/14	cdp stp vtp	//	//	down
pa	gp udld	//	//	
Fa0/15	cdp stp vtp	//	//	down
pa	.gp udld	//	//	
Fa0/16	cdp stp vtp	//	//	down
pa	gp lacp udld	//	//	
Fa0/17	cdp stp vtp	//	//	down
pa	gp lacp udld	//	//	
Switch#				

Related Commands	Command	Description
	l2protocol-tunnel	Enables protocol tunneling on an interface.
	l2protocol-tunnel cos	Configures the class of service (CoS) value for all tunneled
		Layer 2 protocol packets.

show lacp

To display LACP information, use the **show lacp** command.

show lacp [channel-group] {counters | internal | neighbors | sys-id }

		$(0, \mathbf{i})$	al) Numb	er of the	channel	gro	un v	alid	value	s are	from	1 to	64	
Syntax Description	channel-group	(Option	ai) munic			0	Jup, v	anu			nom	1 10	0	
	counters	Display	s the LAC	CP statist	ical info	rma	ation.							
	internal	Display	s the inte	rnal infor	mation.									
	neighbors	Display	s the neig	ghbor info	ormation	۱.								
	sys-id	Display	s the LAC	CP system	n identif	icati	ion.							
Defaults	This commond	haa na dafa	lt cotting											
Delauns	This command	nas no dera	int setting	8.										
Command Modes	Privileged EXE	C mode												
Command History	Release	Modific	ation											
	12.1(13)EW	Suppor	t for this o	command	was int	rodu	uced	on th	e Cat	alyst	4500) serie	es swit	ches.
Usage Guidelines	This command If you do not sp You can enter th	ecify a <i>char</i> ne optional a	nnel-grou	p value, a	ll chann	iel g	group	s are	displ	ayed.				ccept th
	If you do not sp You can enter tl sys-id keyword	ecify a <i>cha</i> n ne optional a	nnel-grou channel-g	p value, a <i>roup</i> valu	ll chann ie to spe	el g	group: 7 a cha	s are	displ grou	ayed.	all k	eywo	rds, e	-
	If you do not sp You can enter th sys-id keyword This example sh	ecify a <i>chan</i> ne optional a	nnel-grou channel-g o display l	p value, a <i>roup</i> valu	ll chann ie to spe	el g	group: 7 a cha	s are	displ grou	ayed.	all k	eywo	rds, e	-
	If you do not sp You can enter tl sys-id keyword	ecify a <i>chan</i> ne optional a	nnel-grou channel-g o display l sters	p value, a <i>roup</i> valu	ll chann ie to spe	nel g cify nfor	group: 7 a cha rmati	s are	displ grou	ayed.	all k	eywo	rds, e	-
	If you do not sp You can enter th sys-id keyword This example sh	ecify a <i>chan</i> ne optional <i>a</i> nows how to acp 1 count LACPDUS	nnel-grou channel-g o display l sters	p value, a roup valu LACP sta	ill chann ie to spe tistical i	nel g cify nfor	group: 7 a cha rmatio	s are	displ grou	ayed.	all k	eywo	rds, e	-
	If you do not sp You can enter th sys-id keyword This example sh Switch# show	ecify a <i>chan</i> ne optional a nows how to acp 1 count LACPDUS Lt Recv	nnel-grou channel-g o display l t ters Ma	p value, a <i>roup</i> valu LACP sta	ll chann te to spe tistical i LACP	nel g cify nfor	group: 7 a cha rmatio	s are	displ grou	ayed.	all k	eywo	rds, e	-
	If you do not sp You can enter th sys-id keyword This example sh Switch# show 1 Port Ser Channel group: Fa4/1 8	ecify a <i>chan</i> ne optional of nows how to acp 1 count LACPDUS at Recv	nnel-grou, channel-g display l sters Ma Sent 	p value, a roup valu LACP sta rker Recv	ll chann le to spe- tistical i LACP Pkts 	nfor DUs Eri 0	rmatio	s are	displ grou	ayed.	all k	eywo	rds, e	-
	If you do not sp You can enter th sys-id keyword This example sh Switch# show D Port Ser Channel group Fa4/1 8 Fa4/2 14	ne optional of nows how to acp 1 count LACPDUS at Recv	nnel-grou, channel-g display l aters Sent 0 0	p value, a roup valu LACP sta rker Recv	tistical i LACP Pkts	nfor DUS	rmatio	s are	displ grou	ayed.	all k	eywo	rds, e	-
	If you do not sp You can enter th sys-id keyword This example sh Switch# show 1 Port Ser Channel group: Fa4/1 8	ecify a <i>chan</i> ne optional of nows how to acp 1 count LACPDUS at Recv	nnel-grou, channel-g display l sters Ma Sent 	p value, a roup valu LACP sta rker Recv	ll chann le to spe- tistical i LACP Pkts 	nfor DUs Eri 0	rmatio	s are	displ grou	ayed.	all k	eywo	rds, e	-
	If you do not sp You can enter th sys-id keyword This example sh Switch# show D Port Ser Channel group Fa4/1 8 Fa4/2 14 Fa4/3 14	ne optional of nows how to acp 1 count LACPDUS at Recv	nnel-grou, channel-g display l aters Ma Sent 0 0 0	p value, a roup valu LACP sta rker Recv	tistical i LACP Pkts 3 3 0	nfor DUs Eri 0	rmatio	s are	displ grou	ayed.	all k	eywo	rds, e	-
	If you do not sp You can enter the sys-id keyword This example sh Switch# show D Port Ser Channel group Fa4/1 8 Fa4/2 14 Fa4/3 14 Fa4/4 13	ne optional of ne optional of nows how to acp 1 count LACPDUS tt Recv 1 15 18 18 18	nnel-grou, channel-g o display l aters Ma Sent 0 0 0 0	p value, a roup valu LACP sta rker Recv	tistical i LACP Pkts	nfor DUs Eri 0	rmatio	s are	displ grou	ayed.	all k	eywo	rds, e	-
Usage Guidelines	If you do not sp You can enter the sys-id keyword This example sh Switch# show D Port Ser Channel group: Fa4/1 8 Fa4/2 14 Fa4/3 14 Fa4/4 13 Switch#	ecify a <i>chan</i> ne optional <i>a</i> nows how to acp 1 count LACPDUS tt Recv 1 15 18 18 18 18	o display l channel-g o display l tters Ma Sent 0 0 0 0 0 0 0 0	p value, a roup valu LACP sta rker Recv 0 0 0 0	tistical i LACP Pkts 0 0	nfor DUs Erri 0	rmati ^r	s are annel	displ grou r a sp	ayed. p for	all k	unnel	rds, er	

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
                       LACPDUs
                                LACP Port
                                            Admin Oper
                                                            Port
                                                                    Port
              State Interval Priority Key
Port
        Flags
                                                     Key
                                                            Number
                                                                    State
               bndl ..
bndl 30s
bndl 30s
-- 30s
Fa4/1
      saC
               bndl 30s 32768
                                             100
                                                     100
                                                            0xc1
                                                                    0x75
                                  32768
                                            100
                                                     100
Fa4/2
     saC
                                                            0xc2
                                                                    0x75
                                  32768
32768
Fa4/3
        saC
                                              100
                                                     100
                                                            0xc3
                                                                    0x75
Fa4/4
        saC
                                              100
                                                     100
                                                            0xc4
                                                                    0x75
Switch#
```

Table 2-22 lists the output field definitions.

Field	Description					
State	State of the specific port at the current moment is displayed; allowed values are as follows:					
	• <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.					
LACPDUs 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]:					
	• bit0 : <i>LACP_Activity</i>					
	• bit1 : LACP_Timeout					
	• bit2: Aggregation					
	• bit3 : Synchronization					
	• bit4 : Collecting					
	• bit5 : <i>Distributing</i>					
	• bit6 : <i>Defaulted</i>					
	• bit7 : <i>Expired</i>					

Table 2-22 show lacp internal	Command Output Fields
-------------------------------	------------------------------

This example shows how to display LACP neighbors information for a specific port channel:

	<pre>show lacp 1 m S - Device se A - Device is</pre>	nds PDUs at					
Channel	group 1 neigh	bors					
	Partner		Partner				
Port	System ID		Port Nu	mber	Age	Flags	
Fa4/1	8000,00b0.c	23e.d84e	0x81		29s	Р	
Fa4/2	8000,00b0.c	23e.d84e	0x82		0s	Р	
Fa4/3	8000,00b0.c	23e.d84e	0x83		0s	Р	
Fa4/4	8000,00b0.c	23e.d84e	0x84		0s	Ρ	
	Port	Admin	Oper	Port			
	Priority	Key	Кеу	Stat	е		
Fa4/1	32768	200	200	0x81			
Fa4/2	32768	200	200	0x81			
Fa4/3	32768	200	200	0x81			
Fa4/4 Switch#	32768	200	200	0x81			

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	Command	Description
	lacp port-priority	Sets the LACP priority for the physical interfaces.
	lacp system-priority	Sets the priority of the system for LACP.

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	interface	(Optional) Specifies the interface type; valid values are ethernet , fastethernet , gigabitethernet , tengigabitethernet , pos , atm , port-channel , and ge-wan .
	interface-number	(Optional) Specifies the port number.
Defaults	This command has a	no default settings.
Command Modes	Privileged EXEC m	ode
Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Usage Guidelines	The valid values for	the port number depend on the chassis used.
Examples	This example shows	s how to display the ACL configuration on interface fast 6/1:
	Interface FastEthe Inbound access	access-group interface fast 6/1 ernet6/1: -list is simple-mac-acl s-list is not set
Related Commands	Command	Description
	access-group mode	e Specifies the override modes (for example, VACL overrides PACL) and the non-override modes (for example, merge or strict 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	mac_addr	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 <i>type</i> are fastethernet , gigabitethernet , and tengigabitethernet			
	protocol protocol	(Optional) Specifies a protocol. See the "Usage Guidelines" section for more information.		
	vlan vlan_id	(Optional) Displays entries for the specific VLAN only; valid values are from 1 to 4094.		
Defaults	This commond has no	default settings		
Delauns	This command has no	default settings.		
Command Modes	Privileged EXEC mod	le		
Command History	Release Mo	odification		
	12.1(8a)EW Su	pport for this command was introduced on the Catalyst 4500 series switch.		
	12.1(12c)EW Ad	ded support for extended VLAN addresses.		
	12.2(25)EW Ad	ded support for the 10-Gigabit Ethernet interface.		
Usage Guidelines	For the MAC address table entries that are used by the routed ports, the routed port name is displayed in the "vlan" column not the internal VLAN number.			
	The keyword definitions for the <i>protocol</i> variable are as follows:			
	• ip specifies the IP protocol.			
	• ipx specifies the IPX protocols.			
		-		
	• assigned specifie	s the assigned protocol entries. e 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

vlan	Entries mac address	type +	protocols	port
1 Fa6/1	0030.94fc.0dff 0030.94fc.0dff 0030.94fc.0dff	static static	<pre>ip, ipx, assigned, other ip, ipx, assigned, other ip, ipx, assigned, other</pre>	Switch Switch

Related Commands C

Command	Description
show mac-address-table aging-time	Displays MAC address table aging information.
show mac-address-table count	Displays the number of entries currently in the MAC address table.
show mac-address-table dynamic	Displays the dynamic MAC address table entries only.
show mac-address-table interface	Displays the MAC address table information for a specific interface.
show mac-address-table multicast	Displays information about the multicast MAC address table.
show mac-address-table protocol	Displays the MAC address table information that is based on the protocol.
show mac-address-table static	Displays the static MAC address table entries only.
show mac-address-table vlan	Displays information about the MAC address table for a specific VLAN.

show mac-address-table aging-time

show mac-address-table multicast

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 vlan_id	(Optional) Specifies a	a VLAN; valid values are from 1 to 4094.			
Defaults	This command	has no default settings.				
Command Modes	Privileged EXE	C mode				
Command History	Release	Modification				
	12.1(8a)EW	Support for this com	mand was introduced on the Catalyst 4500 series switch.			
	12.1(12c)EW	Support for extended	d 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	Command		Description			
	show mac-add	ress-table address	Displays the information about the MAC-address table.			
	show mac-add	ress-table count	Displays the number of entries currently in the MAC address table.			
	show mac-add	ress-table dynamic	Displays the dynamic MAC address table entries only.			
	show mac-add	ress-table interface	Displays the MAC address table information for a specific interface			

table.

Displays information about the multicast MAC address

Command	Description
show mac-address-table protocol	Displays the MAC address table information that is based on the protocol.
show mac-address-table static	Displays the static MAC address table entries only.
show mac-address-table vlan	Displays information about the MAC address table for a specific 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 vlan_id	(Optional) Specifies a	VLAN; valid values are from 1 to 4094.		
Defaults					
Command Modes	Privileged EXEC mode				
Command History	Release	Modification			
	12.1(8a)EW	Support for this comr	nand was introduced on the Catalyst 4500 series switch.		
	12.1(12c)EW	Added support for ex	tended VLAN addresses.		
Examples	This example shows how to display the entry count for a specific VLAN:				
Multicast MAC Address Count: 1			0 d) Count: 0 ned) Count: 1 1 le: 32768 1		
Related Commands	Command		Description		
		ress-table address	Displays the information about the MAC-address table.		
	show mac-add	ress-table aging-time	Displays MAC address table aging information.		
		ress-table dynamic	Displays the dynamic MAC address table entries only.		
	show mac-address-table interface		Displays the MAC address table information for a specific interface.		
	show mac-add	ress-table multicast	Displays information about the multicast MAC address table.		
	show mac-address-table protocol		Displays the MAC address table information that is based on the protocol.		

Command	Description
show mac-address-table static	Displays the static MAC address table entries only.
show mac-address-table vlan	Displays information about the MAC address table for a specific VLAN.

show mac-address-table dynamic

To display the 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	address mac_ad	<i>ddr</i> (Optional) Specifies a 48-bit MAC address; the valid format is H.H.H.			
	interface type s	<i>slot/port</i> (Optional) Specifies an interface to match; valid values for <i>type</i> are fastethernet , gigabitethernet , and tengigabitethernet .			
	protocol protoc	<i>col</i> (Optional) Specifies a protocol. See the "Usage Guidelines" section for more information.			
	vlan vlan_id	(Optional) Displays entries for a specific VLAN; valid values are from 1 to 4094.			
Defaults	This command h	has no default settings.			
Command Modes	Privileged EXEC	C mode			
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.			
	12.2(25)EW	Added support for the 10-Gigabit Ethernet interface.			
Usage Guidelines	The keyword det	finitions for the <i>protocol</i> argument are as follows:			
	 assigned spectrum 	pecifies 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 por number designation (such as, 5/7) to a port group number (such as, Po80).				
		dress table entries that are used by the routed ports, the routed port name is displayed in nn not the internal VLAN number.			

Examples

This example shows how to display all the 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 the dynamic MAC address entries with a specific protocol type (in this case, assigned):

Switch# show mac-address-table dynamic protocol assigned

vlan	Entries 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	Co

Command	Description
show mac-address-table protocol	Displays the MAC address table information that is based on the protocol.
show mac-address-table static	Displays the static MAC address table entries only.
show mac-address-table vlan	Displays information about the MAC address table for a specific 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	type		type; valid bitethernet .	values are ethernet ,	fastethernet, gigabitethernet, and	
	slot/por	t Number	of the slot a	nd port.		
Defaults	This cor	nmand has no d	efault setting	<u>(</u> 8.		
Command Modes	Privilege	ed EXEC mode				
Command History	Release	Modi	fication			
-	12.1(8a))EW Supp	ort for this c	ommand was introdu	aced on the Catalyst 4500 series switcl	h.
		11		r the 10-Gigabit Eth	•	
Usage Guidelines		<u>.</u>	ble entries th	at are used by the rou	ited ports, the routed port name is displ	layed
	For the N the "vlar	MAC address tal n" column not tl	ble entries th ne internal V	at are used by the rou LAN number.		layed
	For the M the "vlan This exa	MAC address tal n" column not tl mple shows how	ble entries the ne internal V v to display	at are used by the rou LAN number. MAC address table i	ited ports, the routed port name is displ	layed
	For the M the "vlar This exa Switch# Unicast vlan	MAC address tal n" column not tl mple shows how show mac-addr Entries mac address	ble entries the ne internal V v to display dess-table i type	at are used by the rou LAN number. MAC address table i nterface fastether protocols	nted ports, the routed port name is displ nformation for a specific interface: met6/16 port	layed
	For the M the "vlar This exa Switch# Unicast vlan	MAC address tal n" column not tl mple shows how show mac-addr Entries mac address	ble entries the ne internal V v to display dess-table i type	at are used by the rou LAN number. MAC address table i nterface fastether protocols	nted ports, the routed port name is displ nformation for a specific interface:	layed
	For the M the "vlar This exa Switch# Unicast vlan 2 2	MAC address tal n" column not tl mple shows how show mac-addr Entries mac address	ble entries the ne internal V v to display dess-table i type 1 dynamic 2 dynamic	at are used by the rou LAN number. MAC address table i nterface fastether protocols	nted ports, the routed port name is displ nformation for a specific interface: met6/16	layed
	For the M the "vlar This exa Switch# Unicast vlan 2 2 2	MAC address tal n" column not tl mple shows how show mac-addr Entries mac address 0000.0000.010 0000.0000.010	ble entries the ne internal V v to display dess-table i type 1 dynamic 2 dynamic 3 dynamic	at are used by the rou LAN number. MAC address table i nterface fastether protocols	nformation for a specific interface: met6/16 port FastEthernet6/16 FastEthernet6/16 FastEthernet6/16 FastEthernet6/16	layed
	For the M the "vlar This exa Switch# Unicast vlan 2 2 2 2 2	MAC address tal n" column not tl mple shows how show mac-addr Entries mac address 0000.0000.010 0000.0000.010 0000.0000.	ble entries the ne internal V v to display dess-table i type dynamic dynamic dynamic dynamic dynamic	at are used by the rou LAN number. MAC address table i nterface fastether protocols	nformation for a specific interface: met6/16 port FastEthernet6/16 FastEthernet6/16 FastEthernet6/16 FastEthernet6/16 FastEthernet6/16	layed
	For the M the "vlar This exa Switch# Unicast vlan 2 2 2	MAC address tal n" column not tl mple shows how show mac-addr Entries mac address 	ble entries the ne internal V v to display dess-table i type dynamic dynamic dynamic dynamic dynamic dynamic dynamic	at are used by the rou LAN number. MAC address table i nterface fastether protocols tother other other other other other other	nformation for a specific interface: met6/16 port FastEthernet6/16 FastEthernet6/16 FastEthernet6/16 FastEthernet6/16 FastEthernet6/16 FastEthernet6/16 FastEthernet6/16	layed
	For the M the "vlan This exa Switch# Unicast vlan 2 2 2 2 2 2 2 2 2 2	MAC address tal n" column not tl mple shows how show mac-addr Entries mac address 	ble entries the ne internal V v to display dess-table i type dynamic dynamic dynamic dynamic dynamic dynamic dynamic	at are used by the rou LAN number. MAC address table i nterface fastether protocols tother other other other other other other	nformation for a specific interface: met6/16 port FastEthernet6/16 FastEthernet6/16 FastEthernet6/16 FastEthernet6/16 FastEthernet6/16	layed
	For the M the "vlar This exa Switch# Unicast vlan 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	MAC address tal n" column not tl mple shows how show mac-addr Entries mac address 	ble entries the ne internal V v to display dess-table i type dynamic dynamic dynamic dynamic dynamic dynamic	at are used by the rou LAN number. MAC address table i nterface fastether protocols tother other other other other other other other	nformation for a specific interface: met6/16 port FastEthernet6/16 FastEthernet6/16 FastEthernet6/16 FastEthernet6/16 FastEthernet6/16 FastEthernet6/16 FastEthernet6/16	layed
Usage Guidelines Examples	For the M the "vlan This exa Switch# Unicast vlan 	MAC address tal n" column not tl mple shows how show mac-addr Entries mac address 	ble entries the ne internal V v to display l ess-table i type dynamic dynamic dynamic dynamic dynamic dynamic dynamic	at are used by the rou LAN number. MAC address table i nterface fastether protocols tother other other other other other other ports	nformation for a specific interface: met6/16 port FastEthernet6/16 FastEthernet6/16 FastEthernet6/16 FastEthernet6/16 FastEthernet6/16 FastEthernet6/16 FastEthernet6/16	layed

Related Commands

Command	Description			
show mac-address-table address	Displays the information about the MAC-address table.			
show mac-address-table aging-time	Displays MAC address table aging information.			
show mac-address-table count	Displays the number of entries currently in the MAC address table.			
show mac-address-table dynamic	Displays the dynamic MAC address table entries only.			
show mac-address-table multicast	Displays information about the multicast MAC address table.			
show mac-address-table protocol	Displays the MAC address table information that is based on the protocol.			
show mac-address-table static	Displays the static MAC address table entries only.			
show mac-address-table vlan	Displays information about the MAC address table for a specific VLAN.			

show mac-address-table multicast

show mac-address-table multicast

To display information about the multicast MAC address table, use the **show mac-address-table multicast** command.

show mac-address-table multicast [count | {igmp-snooping [count]} | {user [count]} |
{vlan vlan_num}]

Syntax Description	count	(Optional) Displays the number of multicast entries.				
	igmp-snooping	(Optional) Displays only the addresses learned by IGMP snooping.				
	user	(Optional) Displays only the user-entered static addresses.				
	vlan vlan_num	(Optional) Displays information for a specific VLAN only; valid values are from 1 to 4094.				
Defaults	This command ha	s no default settings.				
Command Modes	Privileged EXEC	mode				
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		ress table entries that are used by the routed ports, the routed port name is displayed in a not the the internal VLAN number.				
	the "vlan" colum					
Usage Guidelines Examples	the "vlan" column This example sho Switch# show mad Multicast Entrid vlan mac add	n not the the internal VLAN number. ws how to display multicast MAC address table information for a specific VLAN: c-address-table multicast vlan 1 es dress type ports				
	the "vlan" column This example sho Switch# show mad Multicast Entrid vlan mac add	n not the the internal VLAN number. ws how to display multicast MAC address table information for a specific VLAN: c-address-table multicast vlan 1 es dress type ports				
	the "vlan" column This example sho Switch# show made Multicast Entrid vlan mac add 1 ffff.ff: Switch#	n not the the internal VLAN number. ws how to display multicast MAC address table information for a specific VLAN: c-address-table multicast vlan 1 es dress type ports				

Related Commands

Command	Description			
show mac-address-table address	Displays the information about the MAC-address table.			
show mac-address-table aging-time	Displays MAC address table aging information. Displays the number of entries currently in the MAC address table.			
show mac-address-table count				
show mac-address-table dynamic	 Displays the dynamic MAC address table entries only. Displays the MAC address table information for a specific interface. Displays the MAC address table information that is based on the protocol. 			
show mac-address-table interface				
show mac-address-table protocol				
show mac-address-table static	Displays the static MAC address table entries only.			
show mac-address-table vlan	Displays information about the MAC address table for a specific VLAN.			

show mac-address-table notification

To display the MAC address table notification status and history, use the **show mac-address-table notification** command.

show mac-address-table notification [change] [interface [interface-id]] | [mac-move] | [threshold]

	[thresh	10ld]
Syntax Description	change	(Optional) Displays the MAC address change notification status.
-	interface	(Optional) Displays MAC change information for an interfaces.
	interface-id	(Optional) Displays the information for a specific interface. Valid interfaces include physical ports and port channels.
	mac-move	(Optional) Displays MAC move notification status.
	threshold	(Optional) Displays the MAC threshold notification status.
Defaults	This command	has no default settings.
Command Modes	Privileged EXE	.C mode
Command History	Release	Modification
	12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switch.
Usage Guidelines	feature is enabl	nac-address-table notification change command to display whether the MAC change ed or disabled, the MAC change notification interval, the maximum number of entries nistory table, and the history table contents.
		ce keyword to display the flags for all interfaces. If the <i>interface-id</i> is included, only the terface are displayed.
Examples	This example sl	hows how to display all the MAC address notification information:
	MAC Notificati Interval betwee Number of MAC Number of MAC Number of Noti Maximum Number Current Histon MAC Notificati History Table	
	History Index MAC Changed Me Operation: Ado	1, Entry Timestamp 478433, Despatch Timestamp 478433 essage :

```
History Index 2, Entry Timestamp 481834, Despatch Timestamp 481834

MAC Changed Message :

Operation: Added Vlan: 1 MAC Addr: 1234.5678.9ab1 Dot1dBasePort: 323

Operation: Added Vlan: 1 MAC Addr: 1234.5678.9ab2 Dot1dBasePort: 323

Operation: Added Vlan: 1 MAC Addr: 1234.5678.9ab3 Dot1dBasePort: 323

Operation: Added Vlan: 1 MAC Addr: 1234.5678.9ab4 Dot1dBasePort: 323

History Index 3, Entry Timestamp 484334, Despatch Timestamp 484334

MAC Changed Message :

Operation: Deleted Vlan: 1 MAC Addr: 1234.5678.9ab0 Dot1dBasePort: 323

Switch#
```

This example shows how to display the MAC address change status on the FastEthernet interface 7/1:

```
      Switch# show mac-address-table notification change interface FastEthernet 7/1

      MAC Notification Feature is Enabled on the switch

      Interface
      MAC Added Trap MAC Removed Trap

      ------
      ------

      FastEthernet7/1
      Enabled

      Disabled
```

Switch#

This example shows how to display the MAC address move status:

```
Switch# show mac-address-table notification mac-move
MAC Move Notification: Enabled
Switch#
```

This example shows how to display the MAC address table utilization status:

Related Commands

ds	Command	Description
	clear mac-address-table	Clears the address entries from the Layer 2 MAC address table.
	mac-address-table notification	Enables MAC address notification on a switch.
	snmp-server enable traps	Enables SNMP notifications (traps or informs).
	snmp trap mac-notification change	Enables SNMP MAC address notifications.

show mac-address-table protocol

To display the MAC address table information that is based on the protocol, use the **show mac-address-table protocol** command.

show mac-address-table protocol $\{assigned \mid ip \mid ipx \mid other\}$

Syntax Description	assigned	Specifie	s the assign	ned protoco	ol ent	ries.					
	ip	Specifie	s the IP pro	otocol entri	es.						
	ipx	Specifie	s the IPX p	orotocol en	tries.						
	other	Specifie	s the other	protocol er	ntries						
Defaults	This comm	and has no d	afault satti	nas							
Delaults		and has no u	clault setti	iigs.							
Command Modes	Privileged H	EXEC mode									
Command History	Release	Modi	fication								
	12.1(8a)EW	V Supp	ort for this	command	was	introduce	ed on the	Cataly	st 4500	series sw	itch.
Hanna Quidalinaa	E. d. MA		1	(1	11	1	1	1	1		•
	the "vlan" c	C address tal column not th le shows how ssigned):	he the inter	nal VLAN	num	ber.	-		-		
	the "vlan" c This examp this case, as	olumn not tl le shows how	he the inter v to display	rnal VLAN y the MAC	addre	ber. ess table e	-		-		
	the "vlan" c This examp this case, as Switch# sh vlan mac	column not the shows how signed):	he the inter w to display ress-table type	y the MAC protocol	num addre assi	ber. ess table e gneđ	entries th	nat have	-		
	the "vlan" c This examp this case, as Switch# sh vlan mac	column not the shows how ssigned):	he the inter w to display ress-table type	y the MAC protocol	addre assi qos	ber. ess table e gneđ	entries th	nat have	-		
	the "vlan" c This examp this case, as Switch# sh vlan mac 200 0050 100 0050	eolumn not the shows how signed): ow mac-addr address 	w to display ress-table type +	y the MAC protocol protocol assigned assigned	addro assi qos -+	ber. ess table o gned 	entries th	nat have	-		
	the "vlan" c This examp this case, as Switch# sh vlan mac 200 0050 100 0050 5 0050	eolumn not the shows how signed): ow mac-addr address 	w to display ress-table type +	y the MAC protocol protocol assigned assigned	addro assi qos 	ber. ess table o gned Switch Switch Switch	entries th	nat have	-		
	the "vlan" c This examp this case, as Switch# sh vlan mac 200 0050 100 0050 5 0050 4092 0000	column not the shows how signed): cow mac-addr address 	v to display v to display type type tatic static static dynamic	y the MAC protocol protocol assigned assigned assigned	addro assi qos -+ 	ber. ess table of gned switch Switch Switch Switch Switch	entries th	nat have	-		
	the "vlan" c This examp this case, as Switch# sh vlan mac 200 0050 100 0050 5 0050 4092 0000 1 0050	eolumn not the shows how signed): ow mac-addr address 	w to display ress-table type +	y the MAC protocol protocol assigned assigned	addro assi qos 	ber. ess table of gned switch Switch Switch Switch Switch Switch	entries th	nat have	-		
	the "vlan" c This examp this case, as Switch# sh vlan mac 	column not the shows how signed): cow mac-address address 	v to display v to display type type tatic static static dynamic static	y the MAC protocol protocol assigned assigned assigned assigned	addro assi qos 	ber. ess table of gned switch Switch Switch Switch Switch Switch	entries th	nat have	-		
	the "vlan" c This examp this case, as Switch# sh vlan mac 200 0050 100 0050 5 0050 4092 0000 1 0050 4 0050 4092 0050 4092 0050	le shows how ssigned): ow mac-addr address 	v to display v to display	y the MAC protocol protocol assigned assigned assigned assigned assigned assigned assigned	addro assi qos 	ber. ess table of gned + Switch Switch Switch Switch Switch Switch Switch Switch Switch	entries th	nat have	-		
Usage Guidelines Examples	the "vlan" c This examp this case, as Switch# sh vlan mac 200 0050 100 0050 5 0050 4092 0000 1 0050 4 0050 4092 0050 4092 0050	column not the shows how asigned): cow mac-address .3e8d.6400 .3e8d.6400 .3e8d.6400 .3e8d.6400 .3e8d.6400 .3e8d.6400 .3e8d.6400 .3e8d.6400 .3e8d.6400 .3e8d.6400	type static static dynamic static static static static	y the MAC protocol protocol assigned assigned assigned assigned assigned	addro assi qos 	ber. ess table of gned + Switch Switch Switch Switch Switch Switch Switch Switch	entries th	nat have	-		

	1	-					
	show mac-address-table protocol other						
	Entries						
	mac address		protocols ++	port			
	0000.0000.0201			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			
	st Entries						
	mac address		-				
1	ffff.fff.ffff	-	Switch,Fa6/15				
	ffff.ffff.ffff	system H	Fa6/16				
	ffff.fff.ffff	system					
	ffff.ffff.ffff	system					
1004	ffff.fff.ffff	system					
1005	ffff.fff.ffff	system					
Fa6/1	ffff.fff.ffff	system S	Switch,Fa6/1				
Fa6/2	ffff.ffff.ffff	system §	Switch,Fa6/2				
Switch#							

This example shows the other output for the previous example:

Related	Commands	(

Command	Description
show mac-address-table address	Displays the information about the MAC-address table.
show mac-address-table aging-time	Displays MAC address table aging information.
show mac-address-table count	Displays the number of entries currently in the MAC address table.
show mac-address-table dynamic	Displays the dynamic MAC address table entries only.
show mac-address-table interface	Displays the MAC address table information for a specific interface.
show mac-address-table multicast	Displays information about the multicast MAC address table.
show mac-address-table static	Displays the static MAC address table entries only.
show mac-address-table vlan	Displays information about the MAC address table for a specific VLAN.

show mac-address-table static

show mac-address-table static

To display the 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	address mac_ad	<i>dr</i> (Optional) Specifies a 48-bit MAC address to match; the valid format is
Syntax Description	address mac_aa	H.H.H.
	interface type na	
		fastethernet, gigabitethernet, and tengigabitethernet.
	protocol protoco	<i>ol</i> (Optional) Specifies a protocol. See the "Usage Guidelines" section for more information.
	vlan vlan_id	(Optional) Displays the entries for a specific VLAN; valid values are from 1 to 4094.
Defaults	This command h	as no default settings.
Command Modes	Privileged EXEC	mode
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.
	12.2(25)EW	Added support for the 10-Gigabit Ethernet interface.
Usage Guidelines		ress table entries that are used by the routed ports, the routed port name is displayed in n not the internal VLAN number.
Usage Guidelines	the "vlan" colum	n not the internal VLAN number.
Usage Guidelines	the "vlan" colum The keyword def	n not the internal VLAN number. initions for the <i>protocol</i> argument are as follows:
Usage Guidelines	the "vlan" colum The keyword def • assigned spe	n not the internal VLAN number. initions for the <i>protocol</i> argument are as follows: ecifies the assigned protocol entries.
Usage Guidelines	 the "vlan" colum The keyword def assigned spe ip specifies t 	n not the internal VLAN number. initions for the <i>protocol</i> argument are as follows: crifies the assigned protocol entries. he IP protocol.
Usage Guidelines	 the "vlan" colum The keyword def assigned spe ip specifies t ipx specifies 	n not the internal VLAN number. initions for the <i>protocol</i> argument are as follows: ecifies the assigned protocol entries.

Examples

This example shows how to display all the static MAC address entries:

Switch# show mac-address-table static

```
Unicast Entries
                         protocols
vlan mac address
                type
                                          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
_____+
   ffff.ffff.ffff system Switch,Fa6/15
 1
 2
    ffff.ffff.ffff system Fa6/16
1002 ffff.ffff.system
1003 ffff.ffff system
1004 ffff.ffff.ffff system
    ffff.ffff.ffff system
1005
                system Switch,Fa6/1
     ffff.fff.ffff
Fa6/1
Fa6/2
    ffff.ffff.ffff system Switch,Fa6/2
.
Switch#
```

This example shows how to display the static MAC address entries with a specific protocol type (in this case, assigned):

```
Switch# show mac-address-table static protocol assigned
```

			protocols	port
	0030.94fc.0dff 0030.94fc.0dff	static	ip,ipx,assigned,other ip,ipx,assigned,other	Switch
Fa6/2	0030.94fc.0dff	static	ip, ipx, assigned, other	Switch
Multica	st Entries			
vlan	mac address	type	ports	
	+	++		
1	ffff.fff.ffff	system \$	Switch,Fa6/15	
2	ffff.fff.ffff	system 1	Fa6/16	
1002	ffff.fff.ffff	system		
1003	ffff.fff.ffff	system		
1004	ffff.fff.ffff	system		
1005	ffff.fff.ffff	system		
Fa6/1	ffff.fff.ffff	system \$	Switch,Fa6/1	
Fa6/2 Switch#	ffff.fff.ffff	system S	Switch,Fa6/2	

Related Commands	Command	Description
	show mac-address-table address	Displays the information about the MAC-address table.
	show mac-address-table aging-time	Displays MAC address table aging information.
	show mac-address-table count	Displays the number of entries currently in the MAC address table.
	show mac-address-table dynamic	Displays the dynamic MAC address table entries only.
	show mac-address-table interface	Displays the MAC address table information for a specific interface.
Command	Description	
----------------------------------	---	
show mac-address-table multicast	Displays information about the multicast MAC address table.	
show mac-address-table protocol	Displays the MAC address table information that is based on the protocol.	
show mac-address-table vlan	Displays information about the MAC address table for a specific VLAN.	

show mac-address-table vlan

To display information about the MAC address table for a specific VLAN, use the **show mac-address-table vlan** command.

show mac-address-table [vlan vlan_id] [protocol protocol]

Syntax Description	vlan vlan_id	(Optional) Displays the entries for a specific VLAN; valid values are from 1 to 4094.
	protocol protoco	<i>l</i> (Optional) Specifies a protocol. See the "Usage Guidelines" section for more information.
Defaults	This command ha	s no default settings.
Command Modes	Privileged EXEC	mode
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		ress table entries used by the routed ports, the routed port name is displayed in the the internal VLAN number.
	The keyword defi	nitions for the <i>protocol</i> variable are as follows:
	•	cifies the assigned protocol entries.
	0 1	ne IP protocol.
	• •	the IPX protocols.
	• Ipx specifies	the If A protocols.
	41 1.01	es the other protocol entries.

Examples This example shows how to display information about the MAC address table 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 0030.94fc.0dff static ip, ipx, assigned, other Switch 1 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 system Switch, Fa6/15
Switch#
```

Related Commands

Command	Description
show mac-address-table address	Displays the information about the MAC-address table.
show mac-address-table aging-time	Displays MAC address table aging information.
show mac-address-table count	Displays the number of entries currently in the MAC address table.
show mac-address-table dynamic	Displays the dynamic MAC address table entries only.
show mac-address-table interface	Displays the MAC address table information for a specific interface.
show mac-address-table multicast	Displays information about the multicast MAC address table.
show mac-address-table protocol	Displays the MAC address table information that is based on the protocol.
show mac-address-table static	Displays the static MAC address table entries only.

show module

To display information about the module, use the **show module** command.

show module [mod | all]

Syntax Description	mod	(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 EXE	C mode
Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(25)EW	Enhanced the output of the show idprom interface command to include the 10-Gigabit Ethernet interface.
Usage Guidelines	supervisor engi If the PoE cons "Status" display	-Module fields in the command output, the show module command displays the ne number but appends the uplink daughter card's module type and information. umed by the module is more than 50 W above the administratively allocated PoE, the ys as "PwrOver." If the PoE consumed by the module is more than 50 W above the PoE ne "Status" displays as "PwrFault."

Switch# show module

Examples

This example shows how to display information for all the 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."

	l Ports	low module a Card Type				lel		erial No.
1 2 3	2 6	•	(- · · /		WS WS	 -X4014 -X4306 -X4418	J2 0(AB054109GH 0000110 AB025104WK
5 6	0 48	Not enoug 10/100Base	n power for mod eTX (RJ45)	ule		-X4148-FX-MT -X4148		0000000000 AB023402RP
	MAC add			Hw		Sw		Status
			005c.9d1a.f9df					
2	0010.7k	ab.9920 to	0010.7bab.9925	0.2				Ok
3	0050.73	56.2b36 to	0050.7356.2b47	1.0				Ok
5	0001.64	fe.a930 to	0001.64fe.a95f	0.0				PwrDeny
	0050.0f .tch#	10.28b0 to	0050.0f10.28df	1.0				Ok

This example shows how to display information for a specific module:

Switch# show module mod2 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 Model Serial Mod Sub-Module Hw Status __ _____ 2 Policy Feature Card 2WS-F6K-PFC2SAD04440HVU1.02 Cat4k MSFC 2 daughterboardWS-F6K-MSFC2SAD04430J9K1.1 1.0 Ok Ok Switch#

This example shows how to display information for all the modules on the switch:

Chassis Type : WS-C4506 Power consumed by backplane : 0 Watts Mod Ports Card Type Model Serial No. 1 6 XG (X2), 1000BaseX (SFP) Supervisor(ac WS-X4517 3 6 1000BaseX (GBIC) WS-X4306 00000110 M MAC addresses Hw Fw Sw Status 1 0004.dd46.7700 to 0004.dd46.7705 0.0 12.2(20r)EW(12.2(20040513:16 Ok 3 0010.7bab.9920 to 0010.7bab.9925 0.2 Ok Switch#

Γ

show monitor

To display information about the SPAN session, use the show monitor command.

show monitor [session] [range session-range | local | remote | all | session-number] [detail]

Syntax Description	session	(Optional) Displays the SPAN information for a session.
	range	(Optional) Displays information for a range of sessions.
	session-range	(Optional) Specifies a range of sessions.
	local	(Optional) Displays all local SPAN sessions.
	remote	(Optional) Displays the RSPAN source and destination sessions.
	all	(Optional) Displays the SPAN and RSPAN sessions.
	session-number	(Optional) Session number; valid values are from1 to 6.
	detail	(Optional) Displays the detailed SPAN information for a session.
Defaults	The detail keywo	rd only displays lines with a nondefault configuration.
Command Modes	Privileged EXEC	mode
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.
	12.2(20)EW	Added support to display ACLs that are applied to SPAN sessions.
Examples	This example sho Catalyst 4500 seri	
	Switten Biew Mor	
	Session 1	
	 Туре	: Local Session
	Source Ports	:
	Both Destination Port	: Fa6/1
	Encapsulation	
	Encapsulatio	on : Native

Ingress : Disabled Learning : Disabled

: 1

Filter VLANs

IP Access-group : 10

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 the 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
IP Access-group : None
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

ids	Command	Description
	monitor session	Enables the SPAN sessions on interfaces or VLANs.

show pagp

To display information about the port channel, use the **show pagp** command.

show pagp [group-number] {counters | dual-active | internal | neighbor}

	counters		ur) chum	l-group number; valid values are from 1 to	04.
		Specifie	es the traf	c counter information.	
	dual-active	Specifie	es the dua	active information.	
	internal	Specifie	es the PA	P internal information.	
	neighbor	-		P neighbor information.	
Defaults	This command h	as no defau	lt setting		
Command Modes	Privileged EXE	C mode			
Command History	Release	Modifica	tion		
-	12.1(8a)EW	Support	for this co	nmand was introduced on the Catalyst 450	0 series switch.
Examples	This example sh	ows how to	display i	formation about the PAgP counter:	
	Switch# show p			C	
		ormation	Fl		
	Port Sen	t Recv	Sent	Recv	
	Channel group:		0		
	Fa5/4 266 Fa5/5 267		0 0	0	
	Channel group:				
	Fa5/6 289	261	0	0	
	Fa5/7 290 Switch#	261	0	0	
	This example sh	ows how to	display H	gP dual-active information:	

Channel group 30 Dual-Active Partner Partner Partner Port Detect Capable Name Port Version Te3/1 Yes VS1-Reg2 Te1/1/7 1.1 Te4/1 Yes VS1-Reg2 Te2/2/8 1.1 Channel group 32 Dual-Active Partner Partner Partner Port Detect Capable Name Port Version Gi1/43 Yes VS3 Gi1/1/43 1.1 Gi1/44 Yes VS3 Gi1/1/44 1.1 Gi1/45 Yes VS3 Gi1/1/45 1.1 Gi1/46 Yes VS3 Gi2/1/46 1.1 Gi1/47 Yes VS3 Gi2/1/47 1.1 Gi1/48 Yes VS3 Gi2/1/48 1.1 Gi2/3 Yes VS3 Gi1/1/1 1.1 Gi2/4 Yes VS3 Gi2/1/1 1.1 Switch#

This example shows how to display internal PAgP information:

Switch# Flags:	S - Dev	ice is s			. C - De	evice is i	n Consisten	t state.
Timers:			is runn imer is :	5	~ ~		is running. imer is run	ning.
Channel	group 1							
				Hello	Partner	PAgP	Learning	
Port	Flags	State	Timers	Interval	Count	Priority	Method	IfIndx
Fa5/4	SC	U6/S7		30s	1	128	Any	129
Fa5/5 Switch#	SC	U6/S7		30s	1	128	Any	129

This example shows how to display PAgP neighbor information for all neighbors:

Flags:	show pagp neighbor S - Device is sending A - Device is in Auto		Device is in Device learn			
Channel g	group 1 neighbors					
	Partner	Partner	Partner		Partner	Group
Port	Name	Device ID	Port	Age	Flags	Cap.
Fa5/4	JAB031301	0050.0f10.230c	2/45	2s	SAC	2D
Fa5/5	JAB031301	0050.0f10.230c	2/46	27s	SAC	2D
Channel g	group 2 neighbors					
	Partner	Partner	Partner		Partner	Group
Port	Name	Device ID	Port	Age	Flags	Cap.
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

mmands	Command	Description	
	pagp learn-method	Learns the input interface of the incoming packets.	
	pagp port-priority	Selects a port in hot standby mode.	

show policy-map

To display information about the policy map, use the show policy-map command.

show policy-map [policy_map_name]

Syntax Description policy_map_name (Optional) Name of the policy map. Defaults This command has no default settings. **Command Modes** Privileged EXEC mode **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 the policy maps: Switch# show policy-map Policy Map ipp5-policy class ipp5 set ip precedence 6 Switch# This example shows how to display information for a specific policy map: Switch# show policy ipp5-policy Policy Map ipp5-policy class ipp5 set ip precedence 6 Switch# **Related Commands** Command Description class-map Creates a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode policy-map Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode Displays class map information. show class-map Displays the statistics and configurations of the input and show policy-map interface output policies that are attached to an interface.

show policy-map control-plane

To display the configuration either of a class or of all classes for the policy map of a control plane, use the **show policy-map control-plane** command.

show policy-map control-plane [input [class class-name] | [class class-name]]

Syntax Description	input	(Optional) Displays statistics for the attached input policy.			
	class class-name	(Optional) Displays the name of the class.			
Defaults	This command has	no default settings.			
Command Modes	Privileged EXEC m	ıode			
Command History	Release	Modification			
	12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switch.			
Usage Guidelines		ot supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.			
		hap control-plane command displays information for aggregate control-plane of the number or rate of packets that are going to the process level.			
Examples	polices traffic that i	as that the policy map TEST is associated with the control plane. This policy map matches the class-map TEST, while allowing all other traffic (that matches the fault) to go through as is. Table 2-23 describes the fields shown in the display.			
	Switch# show policy-map control-plane				
	Control Plane				
	Service-policy	input: system-cpp-policy			
	0 packets	ystem-cpp-eapol (match-all) ess-group name system-cpp-eapol			
	0 packets	vstem-cpp-bpdu-range (match-all) ess-group name system-cpp-bpdu-range			
	28 packets Match: acce police: Per	vstem-cpp-cdp (match-all) ess-group name system-cpp-cdp c-interface 530 bytes Exceed: 0 bytes			

Class-map: system-cpp-garp (match-all) 0 packets Match: access-group name system-cpp-garp Class-map: system-cpp-sstp (match-all) 0 packets Match: access-group name system-cpp-sstp Class-map: system-cpp-cgmp (match-all) 0 packets Match: access-group name system-cpp-cgmp Class-map: system-cpp-ospf (match-all) 0 packets Match: access-group name system-cpp-ospf Class-map: system-cpp-igmp (match-all) 0 packets Match: access-group name system-cpp-igmp Class-map: system-cpp-pim (match-all) 0 packets Match: access-group name system-cpp-pim Class-map: system-cpp-all-systems-on-subnet (match-all) 0 packets Match: access-group name system-cpp-all-systems-on-subnet Class-map: system-cpp-all-routers-on-subnet (match-all) 0 packets Match: access-group name system-cpp-all-routers-on-subnet Class-map: system-cpp-ripv2 (match-all) 0 packets Match: access-group name system-cpp-ripv2 Class-map: system-cpp-ip-mcast-linklocal (match-all) 0 packets Match: access-group name system-cpp-ip-mcast-linklocal Class-map: system-cpp-dhcp-cs (match-all) 0 packets Match: access-group name system-cpp-dhcp-cs Class-map: system-cpp-dhcp-sc (match-all) 0 packets Match: access-group name system-cpp-dhcp-sc Class-map: system-cpp-dhcp-ss (match-all) 0 packets Match: access-group name system-cpp-dhcp-ss Class-map: class-default (match-any) 0 packets Match: any 0 packets Switch#

	Field	Description		
	Fields Associated with Classes o	r Service Policies		
	Service-policy input	Name of the input service policy that is applied to the control plane. (If configured, this field will also show the output service policy.)		
	Class-map	Class of traffic being displayed. Traffic is displayed for each configured class. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.		
	Match	Match criteria for the specified class of traffic.		
		Note For more information about the variety of match criteria options available, refer to the chapter "Configuring the Modular Quality of Service Command-Line Interface" in the <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> .		
	Fields Associated with Traffic Po	licing		
	police	police command has been configured to enable traffic policing.		
	conformed	Action to be taken on packets conforming to a specified rate; displays the number of packets and bytes on which the action was taken.		
	exceeded	Action to be taken on packets exceeding a specified rate; displays the number of packets and bytes on which the action was taken.		
		Decorintion		
ommands	Command control-plane	Description Enters control-plane configuration mode.		

Table 2-23 show policy-map control-plane Field Descriptions

service-policy input (control-plane) Attaches a policy map to a control plane for aggregate control plane services.

show policy-map interface

To display the statistics and configurations of the input and output policies that are 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 int	terface-number	(Optional) Specifies the Fast Ethernet 802.3 interface.		
		t interface-number	 (Optional) Specifies the Gigabit Ethernet 802.3z interface. (Optional) Specifies the port channel. (Optional) Specifies the VLAN ID; valid values are from 1 to 4094. 		
	port-channel <i>n</i>	-			
	vlan vlan_id				
	input		(Optional) Specifies input policies only.		
	output		(Optional) Specifies output policies only.		
Defaults	This command h	nas no default settings			
Command Modes	Privileged EXE	C mode			
Command History	Release Modification				
	12.1(8a)EW	EW Support for this command was introduced on the Catalyst 4500 series switch.			
	12.1(12c)EW	12.1(12c)EWAdded support for extended VLAN addresses.			
	12.2(25)SGDisplays results for full flow policing.				
Examples	attached to an in		ne statistics and configurations of all input and output policies		
	FastEthernet6/1 service-policy input:ipp5-policy				
	class-map:ipp5 (match-all) 0 packets match:ip precedence 5 set: ip precedence 6				
	class-map: 0 packet match:an		h-any)		

```
service-policy output: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#
```

This example shows how to display the 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#
```

With the following configuration, each flow is policed to a 1000000 bps with an allowed 9000-byte burst value.

```
<u>Note</u>
```

If you use the **match flow ip source-address/destination-address** command, these two flows are consolidated into one flow and they have the same source and destination address.

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) # class-map c1
Switch(config-cmap)# match flow ip source-address ip destination-address ip protocol 14
source-port 14 destination-port
Switch(config-cmap) # exit
Switch(config) # policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# police 1000000 9000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastEthernet 6/1
Switch(config-if)# service-policy input p1
Switch(config-if)# end
Switch# write memory
Switch# show policy-map interface
FastEthernet6/1
class-map c1
   match flow ip source-address ip destination-address ip protocol 14 source-port 14
destination-port
policy-map p1
   class c1
```

Γ

```
police 1000000 bps 9000 byte conform-action transmit exceed-action drop
I.
interface FastEthernet 6/1
 service-policy input p1
Switch# show policy-map p1
  Policy Map p1
   Class c1
      police 1000000 bps 9000 byte conform-action transmit exceed-action drop
Switch# show policy-map interface
FastEthernet6/1
  Service-policy input: p1
   Class-map: c1 (match-all)
     15432182 packets
      Match: flow ip source-address ip destination-address ip protocol 14 source-port 14
destination-port
      police: Per-interface
        Conform: 64995654 bytes Exceed: 2376965424 bytes
    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets
Switch#
```

Related Commands	Command	Description	
	class-map	Creates a class map to be used for matching packets to the class whose name you specify and to be used enter class-map configuration mode.	
	policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.	
	show class-map	Displays class map information.	
	show qos	Displays QoS information.	

show policy-map interface vlan

To show the QoS policy-map information applied to a specific VLAN on an interface, use the **show policy-map interface vlan** command.

show policy-map interface vlan interface-id vlan vlan-id

yntax Description	interface interface-id	d (Optional) Displays QoS policy-map information for a specific interface.			
	vlan vlan-id	(Optional) Displays QoS policy-map information for a specific VLAN.			
ommand Modes	Privileged EXEC mod	de			
ommand History	Release Mo	odification			
	12.1(13)EW Su	pport for this command was introduced on the Catalyst 4500 series switch.			
xamples	Take the following co	onfiguration on a non-Supervisor Engine 6-E as an example:			
	interface GigabitEthernet3/1 vlan-range 20,400 service-policy input p1 vlan-range 300-301 service-policy output p2				
	This example shows how to display policy-map statistics on VLAN 20 on the Gigabit Ethernet 6/1 interface:				
	Switch# show policy-map interface gigabitEthernet 3/1 vlan 20 GigabitEthernet3/1 vlan 20				
	Service-policy input: p1				
	Class-map: class-default (match-any) 0 packets Match: any 0 packets police: Per-interface Conform: 0 bytes Exceed: 0 bytes Switch#				
	Take the following configuration on a non-Supervisor Engine 6-E as an example:				
	interface fastethernet6/1 vlan-range 100 service-policy in p1				
	This example shows h	now to display policy-map statistics on VLAN 100 on the FastEthernet interface			
	Switch#show policy-	map interface fastEthernet 6/1 vlan 100			
	FastEthernet6/1 vlan 100				

```
Service-policy input: p1
```

```
Class-map: c1 (match-all)

0 packets

Match: ip dscp af11 (10)

police: Per-interface

Conform: 0 bytes Exceed: 0 bytes

Class-map: class-default (match-any)

0 packets

Match: any

0 packets

Switch#
```

Take the following configuration on a Supervisor Engine 6-E as an example:

```
interface gigabitethernet3/1
vlan-range 100
service-policy in p1
```

This example shows how to display policy-map statistics on VLAN 100 on the FastEthernet interface:

```
Switch#show policy-map interface gigabitethernet 3/1 vlan 100
GigabitEthernet3/1 vlan 100
   Service-policy input: p1
     Class-map: c1 (match-all)
       0 packets
       Match: ip dscp af11 (10)
       police:
          rate 128000 bps, burst 4000 bytes
           conformed 0 packets, 0 bytes; action:
            transmit
           exceeded 0 packets, 0 bytes; action:
             drop
           conformed 0 bps, exceeded 0 bps
     Class-map: class-default (match-any)
       0 packets
       Match: any
         0 packets
```

Switch#

Related Commands	Command	Description
	service-policy (interface configuration)	Attaches a policy map to an interface.
	show policy-map interface	Displays the statistics and configurations of the input and output policies that are attached to an interface.

OL-16005-01

show port-security

To display the port security settings for an interface or for the switch, use the **show port-security** command.

show port-security [address] [interface interface-id]
[interface port-channel port-channel-number] [vlan vlan-id]

Syntax Description	address	(Optional) Displays all secure MAC addresses for all ports or for a specific port.
	interface interface-id	(Optional) Displays port security settings for a specific interface.
	interface <i>port-channel port channel-number</i>	(Optional) Displays port security for a specific port-channel interface.
	vlan vlan-id	(Optional) Displays port security settings for a specific VLAN.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(18)EW	Support was enhanced to display sticky MAC addresses.
	12.2(25)EWA	Support was enhanced to display settings on a per-VLAN basis.
	12.2(31)SGA	Support was enhanced to display settings on EtherChannel interfaces.

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 or *port-channel-interface* 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.

Sticky MAC addresses are addresses that persist across switch reboots and link flaps.

:20 (traps per second)

Security Action	SecurityViolation (Count)	CurrentAddr (Count)	MaxSecureAddr (Count)	Secure Port
Restrict	0	2	2	 Fa3/1
Restrict	0	2	2	Fa3/2
Shutdowr	0	2	2	Fa3/3
Shutdown	0	2	2	Fa3/4
Shutdowr	0	2	2	Fa3/5
Shutdowr	0	2	2	Fa3/6
Shutdowr	0	2	2	Fa3/7
Shutdowr	0	2	2	Fa3/8
Shutdowr	0	0	1	Fa3/10
Shutdowr	0	0	1	Fa3/11
Restrict	0	0	1	Fa3/12
Shutdowr	0	0	1	Fa3/13
Shutdowr	0	0	1	Fa3/14
Shutdowr	0	0	1	Fa3/15
Shutdowr	0	0	1	Fa3/16
Shutdowr	0	1	3	Po2

Examples

This example shows how to display port security settings for the entire switch:

This example shows how to display port security settings for interface Fast Ethernet port 1:

Switch# show port-security interface fastethernet 5/1

Max Addresses limit in System (excluding one mac per port) :3072

Port Security	:	Enabled
Port Status	:	Secure-up
Violation Mode	:	Shutdown
Aging Time	:	0 mins
Aging Type	:	Absolute
SecureStatic Address Aging	:	Disabled
Maximum MAC Addresses	:	1
Total MAC Addresses	:	1
Configured MAC Addresses	:	0
Sticky MAC Addresses	:	1
Last Source Address	:	0000.0001.001a
Security Violation Count	:	0
Switch#		

Global SNMP trap control for port-security

Switch#

on all switch interfaces:

	Secure Mac Add	ress Table		
Vlan	Mac Address	Туре	Ports	Remaining Ag (mins)
	0000.0001.0000	 SecureConfigured	 Fa3/1	 15 (I)
1	0000.0001.0001	SecureConfigured	Fa3/1	. ,
1	0000.0001.0100	SecureConfigured	Fa3/2	
1	0000.0001.0101	SecureConfigured	Fa3/2	-
1	0000.0001.0200	SecureConfigured	Fa3/3	-
1	0000.0001.0201	SecureConfigured	Fa3/3	-
1	0000.0001.0300	SecureConfigured	Fa3/4	-
1	0000.0001.0301	SecureConfigured	Fa3/4	-
1	0000.0001.1000	SecureDynamic	Fa3/5	-
1	0000.0001.1001	SecureDynamic	Fa3/5	-
1	0000.0001.1100	SecureDynamic	Fa3/6	-
1	0000.0001.1101	SecureDynamic	Fa3/6	-
1	0000.0001.1200	SecureSticky	Fa3/7	-
1	0000.0001.1201	SecureSticky	Fa3/7	-
1	0000.0001.1300	SecureSticky	Fa3/8	-
1	0000.0001.1301	SecureSticky	Fa3/8	-
1	0000.0001.2000	SecureSticky	Po2	-

Max Addresses limit in System (excluding one mac per port) :3072

This example shows how to display the maximum allowed number of secure MAC addresses and the current number of secure MAC addresses on interface Gigabitethernet1/1:

Switch#	show port	-security	interface	gigabitethernet1/1 vlan
Default	maximum:	22		
VLAN M	laximum	Current		
2	22	3		
3	22	3		
4	22	3		
5	22	1		
6	22	2		

This example shows how to display the port security settings on interface Gigabitethernet1/1 for VLANs 2 and 3:

Switch	# show port	-security	interface	gigabitethernet1/1	vlan 2-3
Default	t maximum:	22			
VLAN 1	Maximum	Current			
2	22	3	3		
3	22	3	3		

This example shows how to display all secure MAC addresses configured on interface Gigabitethernet1/1 with aging information for each address.

Switch# show port-security interface gigabitethernet1/1 address

	Secure Mac Add	ress Table		
Vlan	Mac Address	Туре	Ports	Remaining Age(mins)
2	0001.0001.0001	SecureConfigured	Gi1/1	-
2	0001.0001.0002	SecureSticky	Gi1/1	-
3	0001.0001.0001	SecureConfigured	Gi1/1	-
3	0001.0001.0002	SecureSticky	Gi1/1	-
3	0001.0001.0003	SecureSticky	Gi1/1	-
4	0001.0001.0001	SecureConfigured	Gi1/1	-
4	0001.0001.0003	SecureSticky	Gi1/1	-
6	0001.0001.0001	SecureConfigured	Gi1/1	-
6	0001.0001.0002	SecureConfigured	Gi1/1	-

Total Addresses: 12

This example shows how to display all secure MAC addresses configured on VLANs 2 and 3 on interface Gigabitethernet1/1 with aging information for each address:

```
Switch# show port-security interface gigabitethernet1/1 address vlan 2-3
```

	Secure Mac Add	ress Table		
Vlan	Mac Address	Туре	Ports	Remaining Age(mins)
2	0001.0001.0001	SecureConfigured	Gi1/1	_
2	0001.0001.0002	SecureSticky	Gi1/1	-
2	0001.0001.0003	SecureSticky	Gi1/1	-
3	0001.0001.0001	SecureConfigured	Gi1/1	-
3	0001.0001.0002	SecureSticky	Gi1/1	-
3	0001.0001.0003	SecureSticky	Gi1/1	-

Total Addresses: 12

Switch#

This example shows how to display the maximum allowed number of secure MAC addresses and the current number of secure MAC addressees on Fast Ethernet port 1:

Switch# show port-security interface fastethernet5/1 vlan Default maximum: 22 VLAN Maximum Current 2 22 3 3 22 3 5 22 1 6 22 2

Switch#

This example shows how to display the port security settings on Fast Ethernet port 1 for VLANs 2 and 3:

```
Switch# show port-security interface fastethernet5/1 vlan 2-3
Default maximum: 22
VLAN Maximum Current
2 22 3
3 22 3
Switch#
```

This example shows how to display all secure MAC addresses configured on Fast Ethernet port 1 with aging information for each address.

Switch# show port-security interface fastethernet5/1 address

C = =====	10	7	m = 1= 1 =
Secure	Mac	Address	Table

Vlan	Mac Address	Туре	Ports	Remaining Age(mins)
2	0001.0001.0001	SecureConfigured	Gi1/1	-
2	0001.0001.0002	SecureSticky	Gi1/1	-
2	0001.0001.0003	SecureSticky	Gi1/1	-
3	0001.0001.0001	SecureConfigured	Gi1/1	-
3	0001.0001.0002	SecureSticky	Gi1/1	-
3	0001.0001.0003	SecureSticky	Gi1/1	-
4	0001.0001.0001	SecureConfigured	Gi1/1	-
4	0001.0001.0002	SecureSticky	Gi1/1	-
4	0001.0001.0003	SecureSticky	Gi1/1	-
5	0001.0001.0001	SecureConfigured	Gi1/1	-
6	0001.0001.0001	SecureConfigured	Gi1/1	-
6	0001.0001.0002	SecureConfigured	Gi1/1	-

Total Addresses: 12

Switch#

This example shows how to display all secure MAC addresses configured on VLANs 2 and 3 on Fast Ethernet port 1 with aging information for each address:

Switch# show port-security interface fastethernet5/1 address vlan 2-3

Vlan	Mac Address	Туре	Ports	Remaining Age(mins)
2	0001.0001.0001	SecureConfigured	Gi1/1	-
2	0001.0001.0002	SecureSticky	Gi1/1	-
2	0001.0001.0003	SecureSticky	Gi1/1	-
3	0001.0001.0001	SecureConfigured	Gi1/1	-
3	0001.0001.0002	SecureSticky	Gi1/1	-
3	0001.0001.0003	SecureSticky	Gi1/1	-

Total Addresses: 12

Switch#

This example shows how to display all secure MAC addresses configured on all switch interfaces:

Switch#	show port	-sec	curity ad	ldress
	Secure	Mac	Address	Table

/lan	Mac Address	Туре	Ports	Remaining Age (mins)
1	0000.0001.0000	SecureConfigured	Fa3/1	15 (I)
1	0000.0001.0001	SecureConfigured	Fa3/1	14 (I)
1	0000.0001.0100	SecureConfigured	Fa3/2	-
1	0000.0001.0101	SecureConfigured	Fa3/2	-
1	0000.0001.0200	SecureConfigured	Fa3/3	-
1	0000.0001.0201	SecureConfigured	Fa3/3	-
1	0000.0001.0300	SecureConfigured	Fa3/4	-
1	0000.0001.0301	SecureConfigured	Fa3/4	-
1	0000.0001.1000	SecureDynamic	Fa3/5	-
1	0000.0001.1001	SecureDynamic	Fa3/5	-
1	0000.0001.1100	SecureDynamic	Fa3/6	-
1	0000.0001.1101	SecureDynamic	Fa3/6	-
1	0000.0001.1200	SecureSticky	Fa3/7	-
1	0000.0001.1201	SecureSticky	Fa3/7	-
1	0000.0001.1300	SecureSticky	Fa3/8	-
1	0000.0001.1301	SecureSticky	Fa3/8	-

Total Addresses in System (excluding one mac per port) :8 Max Addresses limit in System (excluding one mac per port) :3072 Switch#

This example shows how to display the maximum allowed number of secure MAC addresses and the current number of secure MAC addresses on interface Gigabitethernet1/1:

```
Switch# show port-security interface gigabitethernet1/1 vlan
Default maximum: 22
VLAN Maximum Current
   2
          22
                        3
   3
            22
                        3
   4
            22
                        3
            22
   5
                        1
   6
            22
                        2
```

Switch#

This example shows how to display the port security settings on interface Gigabitethernet1/1 for VLANs 2 and 3:

```
Switch# show port-security interface gigabitethernet1/1 vlan 2-3
Default maximum: 22
VLAN Maximum Current
2 22 3
3 22 3
Switch#
```

This example shows how to display all secure MAC addresses configured on interface Gigabitethernet1/1 with aging information for each address.

Switch# show port-security interface gigabitethernet1/1 address

	Secure Mac Add	ress Table		
Vlan	Mac Address	Туре	Ports	Remaining Age(mins)
2	0001.0001.0001	SecureConfigured	Gi1/1	-
2	0001.0001.0002	SecureSticky	Gi1/1	-
3	0001.0001.0001	SecureConfigured	Gi1/1	-
3	0001.0001.0002	SecureSticky	Gi1/1	-
3	0001.0001.0003	SecureSticky	Gi1/1	-
4	0001.0001.0001	SecureConfigured	Gi1/1	-
4	0001.0001.0003	SecureSticky	Gi1/1	-
6	0001.0001.0001	SecureConfigured	Gi1/1	-
6	0001.0001.0002	SecureConfigured	Gi1/1	-

```
Total Addresses: 12
```

Switch#

This example shows how to display all secure MAC addresses configured on VLANs 2 and 3 on interface Gigabitethernet1/1 with aging information for each address:

```
{\tt Switch}\# show port-security interface gigabitethernet1/1 address vlan 2-3
```

	Secure Mac Add	ress Table			
Vlan	Mac Address	Туре	Ports	Remaining Age(mins)	
2	0001.0001.0001	SecureConfigured	Gi1/1	-	
2	0001.0001.0002	SecureSticky	Gi1/1	_	
2	0001.0001.0003	SecureSticky	Gi1/1	_	
3	0001.0001.0001	SecureConfigured	Gi1/1	_	
3	0001.0001.0002	SecureSticky	Gi1/1	_	
3	0001.0001.0003	SecureSticky	Gi1/1	-	
Total Addresses: 12					

```
Switch#
```

Related Commands	Command	Description	
	switchport port-security	Enables port security on an interface.	

show power

To display information about the power status, use the **show power** command.

show power [available | capabilities | detail | inline {[interface] | consumption default | module
 mod} | module | status | supplies]

Syntax Description	available	(Optional) Displays the available system power.		
	capabilities	(Optional) Displays the individual power supply capabilities.		
	detail	(Optional) Displays detailed information on power resources.		
	inline	(Optional) Displays the PoE status.		
	interface	(Optional) Type of interface; the only valid value is fastethernet .		
	consumption of	default (Optional) Displays the PoE consumption.		
	module mod	(Optional) Displays the PoE consumption for the specified module.		
	module	(Optional) Displays the power consumption for each module.		
	status	(Optional) Displays the 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 EXE	C mode		
Command History	Release	Modification		
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.		
	12.2(25)SG	Displays inline power handling for the Supervisor Engine II-TS.		
Usage Guidelines	-	wice is connected to an interface with external power, the switch does not recognize the b. The Device column in the output of the show power inline command displays as		
	If your port is not capable of supporting Power over Ethernet, you will receive this message:			
	Power over Ethernet not supported on interface Admin			
		er in-line <i>interface</i> <i>module</i> command displays the amount of power that is used to 7960 IP Phone. To view the amount of power requested, use the show cdp neighbors		
	PoE consumption devices attached	PoE consumed by FPGAs and other hardware components on the module the operating on for an 802.3af-compliant module can be nonzero, even when there are no powered d to the module. The operating PoE can vary by as much as 20 W because of fluctuations is consumed by the hardware components.		

Examples

This example shows how to display information about the general power supply:

Switch# Power	show power			Fan	Inline
Supply	Model No	Туре	Status	Sensor	Status
	PWR-C45-2800AC PWR-C45-1000AC		-	•	-
*** Powe	er Supplies of dif	ferent type	have been de	tected**	*
	upplies needed by upplies currently	-			
Power Su	ummary	М	aximum		
(in Wa	tts)	Used Av	ailable		
System 1	Power (12V)	328	1360		
Inline 1	Power (-50V)	0	1400		
Backplan	ne Power (3.3V)	10	40		
Total U: Switch#	sed	338 (not t	o exceed Tota	l Maximu	m Available = 750)

This example shows how to display the amount of available system power:

Switch# show p	ower availa	ble					
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 detailed information for system power.

Switch# Power	show power detail			Fan	Inline
Supply	Model No	Туре	Status	Sensor	Status
PS1	PWR-C45-1400DC	DCSP1400W	good	good	n.a.
PS1-1		12.5A	good		
PS1-2		15.0A	off		
PS1-3		15.0A	off		
PS2	none				

Power supplies needed by system : 1 Power supplies currently available : 1

Power Summary		Maximum
(in Watts)	Used	Available
System Power (12V)	360	360
Inline Power (-50V)	0	0
Backplane Power (3.3V)	0	40
Total	360	400

Module Inline Power Summary (Watts) (12V -> -48V on board conversion) _____ Maximum Mod Used Available _____ ---____ 5 25 1 ____ _____ _ _ _ Watts Used of System Power (12V) currently out of reset in reset Mod Model ----- -----_ _ _ _ _____
 1
 WS-X4013+TS
 180

 2
 WS-X4506-GB-T
 60

 3
 WS-X424-GB-RJ45
 90

 For Trav
 20
 180 180 180 60 20 90 50 - ---30 -- Fan Tray _____ ____ Total 360 330 250 Watts used of Chassis Inline Power (-50V) Inline Power Admin Inline Power Oper PS Device PS Device Mod Model Efficiencv _____ _____ _____ 2 WS-X4506-GB-T 0 0 3 WS-X4424-GB-RJ45 - -0 0 89 --_ _____ _____ _____ Total 0 0 0 0 Watts used of Module Inline Power (12V -> -50V) Inline Power Admin Inline Power Oper Mod Model PS Device PS Device Efficiency _____ _____ _____ _____ 1 WS-X4013+TS 6 5 3 3 90 _____ -----_____ Switch#

This example shows how to display power consumption for the module.

Switch# show power module

Watts	Used of System Power	r (12V)		
Mod	Model	currently	out of reset	in reset
1	WS-X4013+TS	180	180	180
2	WS-X4506-GB-T	60	60	20
3	WS-X4424-GB-RJ45	90	90	50
	Fan Tray	30		
	Total	360	330	250

Watts used of Chassis Inline Power (-50V) Inline Power Admin Inline Power Oper Mod Model PS Device PS Device Efficiency ____ _____ -----_____ 2 WS-X4506-GB-T 0 0 0 0 3 WS-X424-GB-RJ45 - - - -89 _ -----_____ _____ 0 0 0 Total 0 Watts used of Module Inline Power (12V -> -50V) Inline Power Admin Inline Power Oper Mod Model PS Device PS Device Efficiency _____ _____ _____ _____ 6 5 3 3 90 WS-X4013+TS 1 -----_____ _____

Switch#

<u>Note</u>

The "Inline Power Oper" column 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" column 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 po	wer stat	us				
Power						Fan	Inline
Supply	Model N	0	Type	S	Status	Sensor	Status
PS1	PWR-C45	-2800AC	AC 28	00W g	looq	good	good
PS2	PWR-C45	-2800AC	AC 28	00W g	looq	good	good
Power S	upply	Max	Min	Max	Min	Absolute	
(Nos in	Watts)	Inline	Inline	System	n 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				
						15 4	DD			
Fa3/1		on								0
Fa3/2		on				4.0				1
Fa3/3		on					Cisco IP			
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
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 fastethernet3/1
Available:677(w) Used:11(w) Remaining:666(w)
Interface Admin Oper
                     Power(Watts)
                                             Class
                               Device
                 From PS To Device
_____ ____
Fa3/1
    auto on 11.2
                      10.0 Ieee PD
                                             0
Interface AdminPowerMax AdminConsumption
       (Watts) (Watts)
_____ ____
Fa3/1
             15.4
                            10.0
Switch#
```

```
Note
```

When the Supervisor Engine II+TS is used with the 1400 W DC power supply (PWR-C45-1400DC), and only one 12.5 A input of the DC power supply is used, the supervisor engine's power consumption may vary depending on whether there is any linecard inserted at slot 2 and 3, as well as on the type of linecards inserted. This amount varies between 155 W and 330 W. This variability also affects the maximum amount of available supervisor engine inline power, which can also vary from 0 W to 175 W. Therefore, it is possible for a supervisor engine to deny inline power to some connected inline power devices when one or more linecards are inserted into the chassis.

The output of the commands **show power detail** and **show power module** display the supervisor engine's variable power consumption and its inline power summary.

Switch# show power det sh power detail Power	ail		Fan	Inline
Supply Model No	Туре	Status		
PS1 PWR-C45-1400DC				 n.a.
PS1-1	12.5A	good		
PS1-2	15.0A	off		
PS1-3	15.0A	off		
PS2 none				
Power supplies needed i Power supplies current				
Power Summary		Maximum		
(in Watts)	Used	Available		
System Power (12V)				
Inline Power (-50V)		0		
Backplane Power (3.3V)	0	40		
Total	360	400		

lod		imum lable				
L 	5	25				
lod	Model		Used of Sys tly out of			
1	WS-X4013+TS	180	180)	180	
2	WS-X4506-GB-T	60)	20	
3	WS-X4424-GB-RJ45	90	90)	50	
	Fan Tray	30		-		
	Total	360	33)	250	
			ed of Chass: ower Admin			0V)
lod	Model		Device		-	Efficienc
2 3		0	0	0	0 -	89 -
	Total	0	0	0	0	
od	Model	Inline P	ed of Module ower Admin Device	Inline 1	Power Oper	-> -50V) Efficienc
1	T-TC V/012, mC	<i>c</i>				
	WS-X4013+TS	6	5	3	3	90
	ch#sh power module	6	5 	3	3	90
h po	ch#sh power module	Watts	5 Used of Syst tly out of	stem Powe	er (12V)	90
h po od	ch#sh power module ower module	Watts	Used of Sys tly out of	stem Powe reset :	er (12V)	90
h po iod 1	ch#sh power module ower module Model	Watts curren	Used of Sys tly out of 180	stem Powe reset : 	er (12V) in reset	90
h po od 1 2	ch#sh power module ower module Model WS-X4013+TS	Watts curren 180 60 90	Used of Sys tly out of 180 60 90	stem Powe reset : 	er (12V) in reset 180	90
h po iod 1 2	ch#sh power module ower module Model WS-X4013+TS WS-X4506-GB-T	Watts curren 180 60	Used of Sys tly out of 180 60 90	stem Power reset : 	er (12V) in reset 180 20	90
h po iod 1 2	ch#sh power module ower module Model 	Watts curren 180 60 90	Used of Sys tly out of 180 60 90	stem Powe reset : 	er (12V) in reset 180 20 50	90
h po Iod 1	ch#sh power module ower module Model 	Watts curren 180 60 90 30 360 Watts us	Used of Sys tly out of 180 60 90	stem Powe reset : 	er (12V) in reset 180 20 50 250 e Power (-5	
h po iod 1 2 3 	ch#sh power module ower module Model 	Watts curren 180 60 90 30 360 Watts us	Used of Sys tly out of 180 60 90 330 ed of Chass:	stem Powe reset : 	er (12V) in reset 180 20 50 250 e Power (-5	
h po od 1 2 3 	ch#sh power module wer module Model 	Watts curren 180 60 90 30 360 Watts us Inline P PS	Used of Sys tly out of 18(6(9(33) ed of Chass: ower Admin Device	stem Power reset : 	er (12V) in reset 180 20 50 250 e Power (-5 Power Oper Device	 0V) Efficienc
h po od 1 2 3 	ch#sh power module wer module Model 	Watts curren 180 60 90 30 360 Watts us Inline P	Used of Sys tly out of 18(6(9(33) ed of Chass ower Admin	stem Power reset : 	er (12V) in reset 	 0V)
h po od 2 od 2	ch#sh power module wer module Model 	Watts curren 180 60 90 30 360 Watts us Inline P PS	Used of Sys tly out of 18(6(9(33) ed of Chass: ower Admin Device	stem Power reset : 	er (12V) in reset 180 20 50 250 e Power (-5 Power Oper Device	 0V) Efficienc
h po od 1 2 3 	ch#sh power module wer module Model 	Watts curren 180 60 90 30 360 Watts us Inline P PS 0 - - 0	Used of Sys tly out of 	stem Power reset : 	er (12V) in reset 	0V) Efficienc
h po od 1 2 3 	ch#sh power module wer module Model 	Watts curren 180 60 90 30 360 Watts us Inline P PS 0 0 Watts us	Used of Sys tly out of 	stem Powe reset : 	er (12V) in reset 250 e Power (-5) Power Oper Device 	0V) Efficienc
h po lođ 1 2	ch#sh power module wer module Model 	Watts curren 180 60 90 30 360 Watts us Inline P PS 0 0 Watts us	Used of Sys tly out of 	stem Powe reset : 	er (12V) in reset 	0V) Efficienc

Switch#

Related Commands

mmands	Command	Description
	power dc input	Configures the power DC input parameters on the switch.
	power inline	Sets the inline-power state for the inline-power-capable interfaces.
	power inline consumption	Sets the default power that is allocated to an interface for all the inline-power-capable interfaces on the switch.
	power redundancy-mode	Configures the power settings for the chassis.

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 mode

 Release
 Modification

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

Usage Guidelines This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.

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	Command	Description
	qos (global configuration mode)	Globally enables QoS functionality on the switch.
	qos (interface configuration mode)	Enables QoS functionality on an interface.

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	aggregate_nam	<i>ne</i> (Optional) Named aggregate policer.
Defaults	This command	has no default settings.
Command Modes	Privileged EXE	C mode
Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Fxamples		policer name is case sensitive.
Examples	Switch# show q Policer aggr-1 Rate(bps):1000 conform-action Policymaps usi	00000 Normal-Burst(bytes):1000000 n:transmit exceed-action:policed-dscp-transmit ing this policer:
	ipp5-polic Switch#	
Related Commands	Command	Description
	qos aggregate-	-policer Defines a named 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 mode

 Release
 Modification

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

Usage Guidelines This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.

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 14-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
DBL DSCPs with default drop probability:
1-10
Switch#

Related Commands	Command	Description
	qos (global configuration mode)	Globally enables QoS functionality on the switch.
	qos dbl	Enables Dynamic Buffer Limiting (DBL) globally on the switch.

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]

	P 4 41 4 1	1	(
Syntax Description	fastethernet interface-number			Specifies the Fast Ethernet 802.3 interface.		
	gigabitetherne	et interface-nu		-	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>i</i>	number		(Optional) Sp 1 to 64.	becifies the port channel; valid ranges are from	
Defaults	This command	has no default	t settings.			
Command Modes	Privileged EXE	C mode				
Command History	Release	Modificati	on			
	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(13)EW	Added sup	port for extended	nded VLAN	addresses.	
	12.1(13)EW 12.1(19)EW	-	1		addresses. Trust Device.	
Usage Guidelines	12.1(19)EW	Display ch	nanged to incl	lude the Port		
	12.1(19)EW	Display ch	ed on the Sup	lude the Port	Trust Device. ne 6-E and Catalyst 4900M chassis.	
Usage Guidelines Examples	12.1(19)EW This command This example st Switch# show of QoS is ena Port QoS is Administra Operationa Port Trust	Display ch is not support hows how to c gos interface abled globall	anged to incl ed on the Sup lisplay queue a fastethern y rust State: : State: 'un sco-phone'	lude the Port pervisor Engi ing informati et 6/1	Trust Device. ne 6-E and Catalyst 4900M chassis.	
	12.1(19)EW This command This example st Switch# show of QoS is ena Port QoS is Administra Operationa Port Trust	Display ch Display ch is not support hows how to c gos interface abled globall is enabled ative Port Tr al Port Trust t Device: 'cis SCP:0 Default Bandwidth	anged to incl ed on the Sup lisplay queue fastethern y rust State: State: 'un sco-phone' CoS:0 ShapeRate	lude the Port pervisor Engi ing informati et 6/1	Trust Device. ne 6-E and Catalyst 4900M chassis. on: QueueSize	
	12.1(19)EW This command This example si Switch# show of QoS is ena Port QoS i Administra Operationa Port Trust Default DS	Display ch is not support hows how to co gos interface abled globall is enabled ative Port Tr al Port Trust c Device: 'cis SCP:0 Default	anged to incl ed on the Sup lisplay queue fastethern y rust State: State: 'un sco-phone' CoS:0	lude the Port pervisor Engi ing informati et 6/1 `dscp' trusted'	Trust Device. ne 6-E and Catalyst 4900M chassis. on:	
-	12.1(19)EW This command This example so Switch# show of QoS is ena Port QoS is Administra Operationa Port Trust Default DS Tx-Queue	Display ch is not support hows how to co gos interface abled globall is enabled ative Port Tr al Port Trust c Device: 'cis SCP:0 Default Bandwidth (bps) 31250000 31250000	ed on the Sup lisplay queue fastethern y sust State: 'un sco-phone' CoS:0 ShapeRate (bps) disabled disabled	lude the Port pervisor Engi ing informati et 6/1 `dscp' trusted' Priority N/A N/A	Trust Device. ne 6-E and Catalyst 4900M chassis. on: QueueSize (packets) 240 240 240	
-	12.1(19)EW This command This example st Switch# show of QoS is ena Port QoS i Administra Operationa Port Trust Default DS Tx-Queue 1	Display ch is not support hows how to co gos interface abled globall is enabled ative Port Tr al Port Trust c Device: 'cis SCP:0 Default Bandwidth (bps) 31250000	ed on the Sup lisplay queue fastethern y sust State: 'un sco-phone' CoS:0 ShapeRate (bps) disabled	lude the Port pervisor Engi ing informati et 6/1 `dscp' trusted' Priority N/A	Trust Device. ne 6-E and Catalyst 4900M chassis. on: QueueSize (packets) 240	
Related Commands	Command	Description				
------------------	-------------	---				
	qos map cos	Defines the ingress CoS-to-DSCP mapping for the trusted interfaces.				
	show qos	Displays QoS information.				
	tx-queue	Configures the transmit queue parameters for an interface.				

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 comma	nd has no default settings.
Command Modes	Privileged EXEC mode	
Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch
-		nd is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis. e shows how to display QoS map settings:
-	This example Switch# sho DSCP-TxQueu	e shows how to display QoS map settings:
Usage Guidelines Examples	This example Switch# sho DSCP-TxQueu d1 :d2 0	e shows how to display QoS map settings: w qos maps e Mapping Table (dscp = d1d2) 1 2 3 4 5 6 7 8 9
-	This example Switch# sho DSCP-TxQueu d1 :d2 0 0 : 01 0	e shows how to display QoS map settings: w qos maps e Mapping Table (dscp = d1d2)
-	This example Switch# sho DSCP-TxQueu d1 :d2 0 0 : 01 0 1 : 01 0 2 : 02 0	e shows how to display QoS map settings: w qos maps e Mapping Table (dscp = d1d2) 1 2 3 4 5 6 7 8 9
-	This example Switch# sho DSCP-TxQueu d1 :d2 0 0 : 01 0 1 : 01 0 2 : 02 0 3 : 02 0	e shows how to display QoS map settings: w qos maps e Mapping Table (dscp = d1d2) 1 2 3 4 5 6 7 8 9
-	This example Switch# sho DSCP-TxQueu d1 :d2 0 0 : 01 0 1 : 01 0 2 : 02 0 3 : 02 0 4 : 03 0 5 : 04 0	e shows how to display QoS map settings: w qos maps e Mapping Table (dscp = d1d2) 1 2 3 4 5 6 7 8 9
-	This example Switch# sho DSCP-TxQueu d1 :d2 0 0 : 01 0 1 : 01 0 2 : 02 0 3 : 02 0 4 : 03 0 5 : 04 0	e shows how to display QoS map settings: w qos maps e Mapping Table (dscp = d1d2) 1 2 3 4 5 6 7 8 9
-	This example Switch# sho DSCP-TxQueu d1 :d2 0 0 : 01 0 1 : 01 0 2 : 02 0 3 : 02 0 4 : 03 0 5 : 04 0 6 : 04 0 Policed DSC	e shows how to display QoS map settings: w qos maps e Mapping Table (dscp = d1d2) 1 2 3 4 5 6 7 8 9
-	This example Switch# sho DSCP-TxQueu d1 :d2 0 0 : 01 0 1 : 01 0 2 : 02 0 3 : 02 0 4 : 03 0 5 : 04 0 6 : 04 0 Policed DSC d1 :d2 0	<pre>e shows how to display QoS map settings: w qos maps e Mapping Table (dscp = d1d2) 1 2 3 4 5 6 7 8 9 </pre>
-	This example Switch# sho DSCP-TxQueu d1 :d2 0 0 : 01 0 1 : 01 0 2 : 02 0 3 : 02 0 3 : 02 0 4 : 03 0 5 : 04 0 6 : 04 0 Policed DSC d1 :d2 0 0 : 00 0 1 : 10 1	a a b b b a b b b b a b b b b b a b b b b b c a b b c c c c b a b b c c c c c c c a b c
-	This example Switch# sho DSCP-TxQueu d1 :d2 0 0 : 01 0 1 : 01 0 2 : 02 0 3 : 02 0 4 : 03 0 6 : 04 0 Policed DSC d1 :d2 0 0 : 00 0 1 : 10 1 2 : 20 2	<pre>e shows how to display QoS map settings: w qos maps e Mapping Table (dscp = d1d2) 1 2 3 4 5 6 7 8 9 </pre>
-	This example Switch# sho DSCP-TxQueu d1 :d2 0 0 : 01 0 1 : 01 0 2 : 02 0 3 : 02 0 4 : 03 0 5 : 04 0 6 : 04 0 Policed DSC d1 :d2 0 0 : 00 0 1 : 10 1 2 : 20 2 3 : 30 3	a a b b b a b b b b a b b b b b a b b b b b c a b b c c c c b a b b c c c c c c c a b c
-	This example Switch# sho DSCP-TxQueu d1 :d2 0 0 : 01 0 1 : 01 0 2 : 02 0 3 : 02 0 4 : 03 0 5 : 04 0 6 : 04 0 Policed DSC d1 :d2 0 0 : 00 0 1 : 10 1 2 : 20 2 3 : 30 3 4 : 40 4	e shows how to display QoS map settings: w qos maps e Mapping Table (dscp = d1d2) 1 2 3 4 5 6 7 8 9

DSCP-C	CoS Ma	pping	у Та	able	e (c	lscr		d1o	12)	
d1 :d2	2 0	1 2	3	4	5	6	7	8	9	
										-
0 :	00 0	0 0 0	00	00	00	00	00	01	01	
1 :	01 0	1 01	01	01	01	02	02	02	02	
2 :	02 0	2 02	02	03	03	03	03	03	03	
3 :	03 0	3 04	04	04	04	04	04	04	04	
4 :	05 0	5 05	05	05	05	05	05	06	06	
5:	06 0	6 06	06	06	06	07	07	07	07	
6 :	07 0	7 07	07							
CoS-DS	SCP Ma	pping	у Та	able	e					
CoS	S: 0	1 2	2 3	3 4	1 5	56	5 5	7		
DSCI	b: 0	8 10	5 24	1 32	2 40) 48	3 56	5		
Switch	1#									

Related Commands

Command	Description
qos (global configuration mode)	Globally enables QoS functionality on the switch.
qos (interface configuration mode)	Enables QoS functionality on an interface.

show redundancy

To display redundancy facility information, use the **show redundancy** command.

show redundancy {clients | counters | history | states}

Syntax Description	clients	(Optional) Displays information about the redundancy facility client.		
	counters	(Optional) Displays information about the redundancy facility counter.		
	history	(Optional) Displays a log of past status and related information for the redundancy facility.		
	states	(Optional) Displays information about the redundancy facility state, such as disabled initialization, standby, active.		
Defaults	This command l	This command has no default settings.		
Command Modes	Privileged EXE	C mode		
Command History	Release	Modification		
	12.1.(13)EW	Support for this command was introduced on the Catalyst 4500 series switch (Catalyst 4507R only).		
	12.2(31)SGA	Support for ISSU was introduced.		
	Switch# show r Switch# show r 4507r-demo#sho Redundant Syst	edundancy		
	Switch# show r 4507r-demo#sho Redundant Syst 	w redundancy		
	Switch# show r 4507r-demo#sho Redundant Syst 	redundancy w redundancy em Information : 		
	Switch# show r 4507r-demo#sho Redundant Syst 	<pre>redundancy w redundancy em Information :</pre>		

```
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Wed 14-Jul-04 04:42 by esi
                         BOOT = bootflash:cat4000-i5s-mz.122_20_EWA_392,1
       Configuration register = 0x2002
Peer Processor Information :
_____
             Standby Location = slot 2
       Current Software state = STANDBY HOT
       Uptime in current state = 2 days, 2 hours, 39 minutes
                Image Version = Cisco Internetwork Operating System Software
IOS (tm) Catalyst 4000 L3 Switch Software (cat4000-I5S-M), Version 12.2(20)EWA(3
.92), CISCO INTERNAL USE ONLY ENHANCED PRODUCTION VERSION
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Wed 14-Jul-04 0
                         BOOT = bootflash:cat4000-i5s-mz.122_20_EWA_392,1
       Configuration register = 0x2002
```

Switch#

This example shows how to display redundancy facility client information:

Switch# show redundancy clients

clientID =	0	clientSeq = 0	D	RF_INTERNAL_MSG
clientID =	30	clientSeq = 1	135	Redundancy Mode RF
clientID =	28	clientSeq = 3	330	GALIOS_CONFIG_SYNC
clientID =	65000	clientSeq = 6	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
        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
Switch#
```

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) seg=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
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)
Switch#
```

This example shows how to display information about the redundancy facility state:

```
Switch# show redundancy states
my state = 13 -ACTIVE
     peer state = 8 -STANDBY HOT
          Mode = Duplex
           Unit = Primary
        Unit ID = 2
Redundancy Mode (Operational) = Stateful Switchover
Redundancy Mode (Configured) = Stateful Switchover
     Split Mode = Disabled
   Manual Swact = Enabled
 Communications = Up
   client count = 21
 client_notification_TMR = 240000 milliseconds
          keep_alive TMR = 9000 milliseconds
        keep_alive count = 0
    keep_alive threshold = 18
           RF debug mask = 0x0
Switch#
```

Related Commands	Command	Description
	redundancy	Enters the redundancy configuration mode.
	redundancy force-switchover	Forces a switchover from the active to the standby supervisor engine.

show redundancy config-sync

To display an ISSU config-sync failure or the ignored mismatched command list (MCL), if any, use the **show redundancy config-sync** command.

show redundancy config-sync {failures | ignored } {bem | mcl | prc}

show redundancy config-sync ignored failures mcl

Syntax Description	failures	Displays MCL entries or BEM/PRC failures.				
	ignored	Displays the ignored MCL entries.				
	bem	(Deprecated)				
	mcl	Displays commands that exist in the active supervisor engine's running configuration, but are not supported by the image on the standby supervisor engine.				
	prc	Displays a Parser Return Code (PRC) failure and forces the system to operate in RPR mode provided there is a mismatch in the return code for a command execution at the active and standby supervisor engine.				
Defaults	This comman	d has no default settings.				
Command Modes	User EXEC					
Command History	Release	Modification				
	12.2(31)SGA	This command was introduced on the Catalyst 4500 series switch.				
	12.2(44)SG	Updated command syntax from issu config-sync to redundancy config-sync.				
Usage Guidelines	differ. If any o supervisor en syntax check moved into th	rsions of Cisco IOS images are involved, the command sets supported by two images might of those mismatched commands are executed on the active supervisor engine, the standby gine might not recognize those commands. This causes a config mismatch condition. If the for the command fails on standby supervisor engine during a bulk sync, the command is ne MCL and the standby supervisor engine is reset. To display all the mismatched se the show redundancy config-sync failures mcl command.				

To *clean* the MCL, follow these steps:

- **Step 1** Remove all mismatched commands from the active supervisor engines' running configuration.
- **Step 2** Revalidate the MCL with a modified running configuration using the **redundancy config-sync validate mismatched-commands** command.
- **Step 3** Reload the standby supervisor engine.

Alternatively, you could ignore the MCL by following these steps:

- Step 1 Enter the redundancy config-sync ignore mismatched-commands command.
- **Step 2** Reload the standby supervisor engine; the system transitions to SSO mode.



If you ignore the mismatched commands, the *out-of-sync* configuration at the active supervisor engine and the standby supervisor engine still exists.

Step 3 You can verify the ignored MCL with the **show redundancy config-sync ignored mcl** command.

Each command sets a return code in the action function that implements the command. This return code indicates whether or not the command successfully executes. The active supervisor engine maintains the PRC after executing a command. The standby supervisor engine executes the command and sends PRC back to the active supervisor engine. PRC failure occurs if these two PRCs do not match. If a PRC error occurs at the standby supervisor engine either during bulk sync or LBL sync, the standby supervisor engine is reset. To display all PRC failures, use the **show redundancy config-sync failures prc** command.

To display best effort method (BEM) errors, use the **show redundancy config-sync failures bem** command.

 Examples
 The following example shows how to display the ISSU BEM failures:

 Switch# show redundancy config-sync failures bem

 BEM Failed Command List

 The list is Empty

 Switch#

 The following example shows how to display the ISSU MCL failures:

 Switch#

 Mismatched Command List

 The list is Empty

 Switch# show redundancy config-sync failures mcl

 Mismatched Command List

 The list is Empty

 Switch#

L

The following example shows how to display the ISSU PRC failures:

Switch#show redundancy config-sync failures prc
PRC Failed Command List
------interface FastEthernet3/2
! <submode> "interface"
- channel-protocol pagp
! </submode> "interface"

Related Commands

ds	Command	Description
	redundancy config-sync	Moves the active supervisor engine into the Mismatched
	mismatched-commands	Command List (MCL) and resets the standby supervisor
		engine.

show running-config

To display the module status and configuration, use the show running-config command.

show running-config [module slot]

Syntax Description	module <i>slot</i>	(Optional) Specifies the module slot number; valid values are from 1 to 6.
Syntax Description		(Optional) Specifies the module slot number, valid values are from 1 to 0.
Defaults	This command	has no default settings.
Command Modes	Privileged EXE	C mode
Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Usage Guidelines	interfaces com mode displayed The show inter	you might see a difference in the duplex mode displayed when you enter the show mand and the show running-config command. If you do see a difference, the duplex in the show interfaces command is the actual duplex mode that the interface is running. faces command shows the operating mode for an interface, while the show command shows the configured mode for an interface.
	but no configura interface speed i once the speed i	ing-config command output for an interface may display a duplex mode configuration ation for the speed. When no speed is displayed in the output, it indicates that the is configured to be auto and that the duplex mode shown becomes the operational setting s configured to something other than auto. With this configuration, it is possible that the x mode for that interface does not match the duplex mode shown with the show command.
Examples	This example sh	nows how to display the module and status configuration for all modules:
·	Switch# show r	running-config 5-CONFIG_I:Configured from console by consolesh runn
	Current config	uration:3268 bytes
	! version 12.1	
	no service pad	l
		amps debug uptime
		amps log uptime
	ino service pas	sword-encryption
	hostname Switc	h
	!	
	!	
	power supplies 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:

To display information about the standby bootflash file system, use the **show slavebootflash:** command.

show slavebootflash: [all | chips | filesys]

Suntax Description	- 11	(Ontional) Displays all possible Electric formation
Syntax Description		(Optional) Displays all possible Flash information.
		(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.
	Magic Numbe Length Programming File System MONLIB Offs Bad Sector Squeeze Log	<pre>er = 0 LOCK: bootflash r = 6887635 File System Vers = 10000 (1.0) = 1000000 Sector Size = 40000 Algorithm = 39 Erased State = FFFFFFF Offset = 40000 Length = F40000 et = 100 Length = C628 Map Offset = 3FFF8 Length = 8 Offset = F80000 Length = 40000 fer Offset = FC0000 Length = 40000 ectors = 0</pre>
	No Unrecove No Squeeze USAGE INFO: Bytes Used Bad Sectors OK Files Deleted Fil Files w/Err	<pre>red Errors in progress = 917CE8 Bytes Available = 628318 = 0 Spared Sectors = 0 = 2 Bytes = 917BE8 es = 0 Bytes = 0</pre>

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
             D86EE0AD 957CE8 9 7470636 Sep 20 1999 13:48:49 rp.halley
2 .. image
6456088 bytes available (9534696 bytes used)
----- FILE SYSTEM STATUS------
 Device Number = 0
DEVICE INFO BLOCK: bootflash
 Magic Number
                     = 6887635 File System Vers = 10000
                                                          (1.0)
 Length
                     = 1000000 Sector Size = 40000
                                                 = FFFFFFFF
 Programming Algorithm = 39
                                Erased State
 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
                     = 0
 Num Spare Sectors
   Spares:
STATUS INFO:
 Writable
 NO File Open for Write
 Complete Stats
 No Unrecovered Errors
 No Squeeze in progress
USAGE INFO:
               = 917CE8 Bytes Available = 628318
 Bytes Used
 Bad Sectors = 0 Spared Sectors = 0
           = 2
                       Bytes = 917BE8
 OK Files
 Deleted Files = 0 Bytes = 0
Files w/Errors = 0 Bytes = 0
Switch>
```

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.			
	1 image 6375DBB7 A4F144 6 10678468 Nov 09 1999 10:50:42 halley 5705404 bytes available (10678596 bytes used) Switch>				
	Switch# show ******** Inte ATTRIBUTE MEM Config Opti Config Stat Card Status Write Prote Voltage Cnt	<pre>hows how to display Flash chip information: slaveslot0: chips l Series 2+ Status/Register Dump ******* ORY REGISTERS: on Reg (4000): 2 us Reg (4002): 0</pre>			
	Intelligent Compatible	0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 0 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:
  8 : B0B0 B0B0 B0B0 B0B0
                       B0B0 B0B0 B0B0
                                    B0B0
  16 : 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:
  8 : B0B0 B0B0 B0B0 B0B0
                       B0B0 B0B0 B0B0
                                    B0B0
      B0B0 B0B0 B0B0
                   B0B0
                       B0B0
                            B0B0
  16 :
                                B0B0
                                    B0B0
  COMMON MEMORY REGISTERS: Bank 3
 Intelligent ID Code : 8989A0A0
 Compatible Status Reg: 8080
 Global Status Reg: B0B0
 Block Status Regs:
  8 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
                                    B0B0
  16 :
      B0B0 B0B0 B0B0 B0B0
                       B0B0
                            B0B0
                                B0B0
                                    B0B0
  COMMON MEMORY REGISTERS: Bank 4
 Intelligent ID Code : FFFFFFF
  IID Not Intel -- assuming bank not populated
This example shows how to display file system information:
Switch# show slaveslot0: filesys
-----FILE SYSTEM STATUS------
```

```
Device Number = 0
DEVICE INFO BLOCK: slot0
 Magic Number
                      = 6887635 File System Vers = 10000
                                                             (1.0)
                      = 1000000 Sector Size = 20000
 Length
 Programming Algorithm = 4 Erased State
File System Offset = 20000 Length = FA0000
                                                 = FFFFFFFF
                                Length = F568
 MONLIB Offset = 100
 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:
               = 9F365C Bytes Available = 5AC9A4
 Bytes Used
               = 0
 Bad Sectors
                         Spared Sectors = 0
               = 1
                         Bytes = 9F35DC
 OK Files
 Deleted Files = 0
                         Bytes = 0
 Files w/Errors = 0
                         Bytes =
Switch>
```

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.			
	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 ******** Inte ATTRIBUTE MEM Config Opti Config Stat Card Status Write Prote Voltage Cnt	<pre>slot0: chips l Series 2+ Status/Register Dump ******* ORY REGISTERS: on Reg (4000): 2 us Reg (4002): 0</pre>			
	Intelligent Compatible	0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 0 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:
  COMMON MEMORY REGISTERS: Bank 2
 Intelligent ID Code : 8989A0A0
 Compatible Status Reg: 8080
 Global
       Status Reg: B0B0
 Block Status Regs:
  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:
  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 : FFFFFFF
  IID Not Intel -- assuming bank not populated
Switch>
```

This example shows how to display file system information:

```
Switch# show slot0: filesys
-----FILE SYSTEM STATUS------
 Device Number = 0
DEVICE INFO BLOCK: slot0
 Magic Number
                    = 6887635 File System Vers = 10000
                                                         (1.0)
                    = 1000000 Sector Size = 20000
 Length
 Programming Algorithm = 4
                                              = FFFFFFFF
                               Erased State
 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:
              = 9F365C Bytes Available = 5AC9A4
 Bytes Used
 Bad Sectors
              = 0
                       Spared Sectors = 0
              = 1
                       Bytes = 9F35DC
 OK Files
 Deleted Files = 0
                       Bytes = 0
 Files w/Errors = 0
                       Bytes = 0
Switch>
```

OL-16005-01

show spanning-tree

12.2(25)EW

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	bridge_group	(Optional) Specifies the bridge group number; valid values are from 1 to 255.			
	active	(Optional) Displays the spanning-tree information on active interfaces only.			
	backbonefast	(Optional) Displays the spanning-tree BackboneFast status.			
	bridge	(Optional) Displays the bridge status and configuration information.			
	id	(Optional) Name of the bridge.			
	inconsistentports	(Optional) Displays the root inconsistency state.			
	interface type	(Optional) Specifies the interface type and number; valid values are fastethernet , gigabitethernet , tengigabitethernet , port-channel (1 to 64), and vlan (1 to 4094).			
	root	(Optional) Displays the 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 the spanning-tree UplinkFast status. (Optional) Specifies the VLAN ID; valid values are from 1 to 4094.			
	vlan vlan_id				
	pathcost method	od (Optional) Displays the default path cost calculation method used.			
	detail	(Optional) Displays a summary of interface information.			
Defaults	Interface informati	on summary is displayed.			
Command Modes	Privileged EXEC r	node			
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.			

Added support for the 10-Gigabit Ethernet interface.

2-633

Examples	This example shows how to display spanning-tree information on the active interfaces only:				
	Switch# show spanning-tree active UplinkFast is disabled BackboneFast is disabled				
	<pre>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</pre>				
	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 the 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
                     0050.3e8d.6402
           Address
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
VLAN3
 Bridge ID Priority 32768
                     0050.3e8d.6403
           Address
            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

	ree enabled protocol ieee 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 Address 0030.94fc.0a00 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Aging Time 300
Interface	Designated
Name	Port ID Prio Cost Sts Cost Bridge ID Port ID
FastEthernet	6/15 129.79 128 19 FWD 0 32768 0030.94fc.0a00 129.79
VLAN2	
Spanning t	ree 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	Designated
Name	Port ID Prio Cost Sts Cost Bridge ID Port ID
 FastEthernet Switch#	6/16 129.80 128 19 FWD 0 32768 0030.94fc.0a01 129.80

This example shows how to display spanning-tree information for Fast Ethernet interface 5/9:

```
Switch# show spanning-tree interface fastethernet5/9
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
Switch#
```

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
Switch#
```

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	Listenir	ng Learnir	ng Forwardi	ng STP Active
vlan1 VLAN2		0 0	0 0	0	1 1	1 1
Switch#	2 VLANs 0	0)	0	2	2

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#

Related Commands Command Description spanning-tree backbonefast Enables BackboneFast on a spanning-tree VLAN. spanning-tree cost Calculates the path cost of STP on an interface. spanning-tree guard Enables root guard. spanning-tree pathcost method Sets the path cost calculation method. Enables PortFast by default on all access ports. spanning-tree portfast default spanning-tree portfast (interface Enables PortFast mode. configuration mode) spanning-tree port-priority Prioritizes an interface when two bridges compete for position as the root bridge. spanning-tree uplinkfast Enables the UplinkFast feature. Configures STP on a per-VLAN basis. 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.		
Syntax Description				
	instance-id	(Optional) Instance identification number; valid values are from 0 to 15.		
	detail	(Optional) Displays detailed MST protocol information.		
	interface interface	(Optional) Interface type and number; valid values for type are fastethernet , gigabitethernet , tengigabitethernet , port-channel , and vlan . See the "Usage Guidelines" section for more information.		
Defaults	This command has n	o default settings.		
Command Modes	Privileged EXEC mo	de		
Command History	Release	Modification		
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.		
	12.2(25)EW	Added support for the 10-Gigabit Ethernet interface.		
Usage Guidelines	This command is not	supported on systems that are configured with a Supervisor Engine I.		
	In the output display of display. This message primary VLAN. The	of the show spanning-tree mst configuration command, a warning message might e appears if you do not map secondary VLANs to the same instance as the associated display includes a list of the secondary VLANs that are not mapped to the same iated primary VLAN. The warning message is as follows:		
	These secondary vlans are not mapped to the same instance as their primary: -> 3			
		and are not mapped to the bank indeance ab their primary.		

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

-------

Switch#
```

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 fastethernet4/1 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	Command	Description
	spanning-tree mst	Sets the path cost and port-priority parameters for any MST instance.
	spanning-tree mst forward-time	Sets the forward delay timer for all the instances.
	spanning-tree mst hello-time	Sets the hello-time delay timer for all the instances.
	spanning-tree mst max-hops	Specifies the number of possible hops in the region before a BPDU is discarded.
	spanning-tree mst root	Designates the primary root.

show storm-control

To display the broadcast storm control settings on the switch or on the specified interface, use the **show storm-control** command.

show storm-control [interface-id | broadcast]

Supervisor Engine 6-E and Catalyst 4900M chassis

show storm-control [interface-id | broadcast | multicast]

Syntax Description	interface-id	(Optio	nal) Specifies	s the inte	rface ID for	r the physical	port.	
	broadcast	(Optio	nal) Displays	s the broa	dcast storm	n threshold set	ting.	
	multicast	(Optio	nal) Displays	s the mult	icast storm	threshold set	ting.	
Command Modes	Privileged EXE	EC mode						
command History	Release	N	lodification					
	12.1(19)EW	S	upport for thi	is comma	nd was intro	oduced on the	Catalyst 450	00 series switch
	12.2(25)EW	A	dded support	t for the	0-Gigabit	Ethernet inter	face.	
	12.2(40)SG	A	dded support	t for the S	Supervisor	Engine 6-E an	d Catalyst 4	900M chassis.
	If you do not er on the switch.						•	cified interface
xamples	If you do not er on the switch. This is an exan	nter an interf nple of outpu	ace ID, the so t from the sh	ettings ar	e displayed n-control c	for the broad	cast traffic t n no keywor	ype for all por ds are entered.
xamples	If you do not er on the switch. This is an exan Because no trat Switch# show Interface Fi	nter an interf nple of outpu ffic type keyv storm-contr lter State	ace ID, the so t from the sh word was enta ol Upper I	ettings ar now storn tered, the Lower	e displayed n-control c broadcast s Current	for the broad	cast traffic t n no keywor	ype for all por ds are entered.
xamples	If you do not er on the switch. This is an exan Because no trai Switch# show Interface Fi	nter an interf nple of outpu ffic type keyv storm-contr lter State	ace ID, the so t from the sh word was enta ol Upper I	ettings ar now storn tered, the	e displayed n-control c broadcast s	for the broad	cast traffic t n no keywor	ype for all port
xamples	If you do not er on the switch. This is an exan Because no trai Switch# show Interface Fi 	nter an interf nple of outpu ffic type keyv storm-contr lter State orwarding prwarding	t from the sh word was entable ol Upper I 30.00% 30.00%	ettings ar now storn tered, the Lower 30.00% 30.00%	e displayed n-control c broadcast s Current 	for the broad	cast traffic t n no keywor	ype for all port
xamples	If you do not er on the switch. This is an exan Because no trai Switch# show Interface Fi 	nter an interf nple of outpu ffic type keyv storm-contr lter State	t from the sh word was entron ol Upper I 	ettings ar now storn tered, the Lower 30.00%	e displayed n-control c broadcast s Current N/A	for the broad	cast traffic t n no keywor	ype for all por
xamples	If you do not er on the switch. This is an exam Because no trai Switch# show Interface Fi 	nter an interf nple of outpu ffic type keyv storm-contr lter State orwarding prwarding	t from the sh word was enter ol Upper I 30.00% 30.00% 30.00%	ettings ar now storn tered, the Lower 30.00% 30.00% 30.00%	e displayed n-control c broadcast s Current N/A N/A N/A	ommand whe	cast traffic t	ype for all por ds are entered. displayed.
xamples	If you do not er on the switch. This is an exam Because no trat Switch# show Interface Fi 	nter an interf	t from the sh word was enter ol Upper I 30.00% 30.00% 30.00%	ettings an now storn tered, the Lower 30.00% 30.00% 30.00%	e displayed n-control c broadcast s Current N/A N/A N/A n-control n	ommand whe	cast traffic t	ype for all por ds are entered. displayed.
xamples	If you do not er on the switch. This is an exam Because no trai Switch# show Interface Fi Gi2/1 Fo Gi4/1 Fo Gi4/1 Fo Gi4/3 Fo Switch# This is an exam Engine 6-E. Switch# show st Interface Fil	nter an interf nple of outpu ffic type keyv storm-contr lter State orwarding orwarding orwarding nple of outpu torm-control mu	t from the sh word was entro ol Upper I 30.00% 30.00% 30.00% t from the sh elticast //Super	ettings an now storn tered, the Lower 30.00% 30.00% 30.00% now storn	e displayed n-control c broadcast s Current N/A N/A N/A n-control n ngine 6-E Level	ommand whe	cast traffic t	ype for all por ds are entered. displayed.

This is an example of output from the **show storm-control** command on a Supervisor Engine 6-E when no keywords are entered.

This is an example of output from the show storm-control command for a specified interface.

Table 2-24

This is an example of output from the **show storm-control** command for a specified interface on a Supervisor Engine 6-E.

```
Switch# show storm-control interface fastethernet6/1Interface Filter State Broadcast Multicast Level------Fa6/1BlockingEnabledDisabledSwitch#
```

Table 2-24 describes the fields in the show storm-control display.

Field	Description	

show storm-control Field Descriptions

Field	Description
Interface	Displays the ID of the interface.
Filter State	Displays the status of the filter:
	• Blocking—Storm control is enabled, and a storm has occurred.
	• Forwarding—Storm control is enabled, and no storms have occurred.
	• Inactive—Storm control is disabled.
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 valid only when storm control is enabled.
	Note N/A is displayed for interfaces that do storm control in the hardware.

Related Commands

Command	Description
storm-control	Enables broadcast storm control on a port and specifies what to do when a storm occurs on a port.
show interfaces counters	Displays the traffic on the physical interface.
show running-config	Displays the running configuration of a switch.

show system mtu

To display the global MTU setting, use the **show system mtu** command.

	show system	m mtu				
Syntax Description	This command has no arguments or keywords.					
Defaults	This command h	has no default settings.				
Command Modes	Privileged EXE	C mode				
Command History	Release 12.1(12c)EW	Modification Support for this command was introduced on the Catalyst 4500 series switch.				
Examples	Switch# show s	nows how to display the global MTU setting: System mtu et MTU is 1550 bytes.				
Related Commands	Command	Description				
	system mtu	Sets the maximum Layer 2 or Layer 3 payload size.				

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]

	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						
	page						
Defaults	The defaults ar	e as follows:					
	• Outputs are displayed without page breaks.						
	Passwords	and other security information are removed from the output.					
Command Modes	Privileged EXI	EC mode					
Command History	Release	Modification					
command mistory	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.					
	12.1(0a)LW	Support for this command was introduced on the Catalyst 4500 series switch.					
Usage Guidelines	Output from th	e show tech-support command may be terminated in midstream with the key					
Usage Guidennes	combination C	trl+Alt+6. The command output is buffered so that the command terminates when output					
	of the current s	sub-command running under this command completes.					
	Press the Retu	sub-command running under this command completes. rn key to display the next line of output, or press the Space bar to display the next page If you do not enter the page keyword, the output scrolls. It does not stop for page breaks.					
	Press the Retu of information.	rn key to display the next line of output, or press the Space bar to display the next page					
	Press the Retu of information. If you enter the in the output. If you do not en	rn key to display the next line of output, or press the Space bar to display the next page If you do not enter the page keyword, the output scrolls. It does not stop for page breaks.					
	Press the Retu of information. If you enter the in the output. If you do not en output are repl The show tech	 rn key to display the next line of output, or press the Space bar to display the next page. If you do not enter the page keyword, the output scrolls. It does not stop for page breaks. password keyword, password encryption is enabled, but only the encrypted form appears there the password keyword, the passwords and other security-sensitive information in the aced in the output with the word "removed." -support commands are a compilation of several show commands and the output can be for a sample display of the output of the show tech-support command, see the individual 					
	Press the Retu of information. If you enter the in the output. If you do not en output are repl The show tech quite lengthy. If show command	 rn key to display the next line of output, or press the Space bar to display the next page If you do not enter the page keyword, the output scrolls. It does not stop for page breaks. password keyword, password encryption is enabled, but only the encrypted form appears there the password keyword, the passwords and other security-sensitive information in the aced in the output with the word "removed." -support commands are a compilation of several show commands and the output can be For a sample display of the output of the show tech-support command, see the individual d listed. e show tech-support command without arguments, the output displays the equivalent of 					
	Press the Retu of information. If you enter the in the output. If you do not er output are repl The show tech quite lengthy. F show command If you enter the	 rn key to display the next line of output, or press the Space bar to display the next page If you do not enter the page keyword, the output scrolls. It does not stop for page breaks. password keyword, password encryption is enabled, but only the encrypted form appears there the password keyword, the passwords and other security-sensitive information in the aced in the output with the word "removed." -support commands are a compilation of several show commands and the output can be For a sample display of the output of the show tech-support command, see the individual d listed. e show tech-support command without arguments, the output displays the equivalent of mmands: 					
	Press the Retu of information. If you enter the in the output. If you do not er output are repl The show tech quite lengthy. F show command If you enter the these show cor	 rn key to display the next line of output, or press the Space bar to display the next page If you do not enter the page keyword, the output scrolls. It does not stop for page breaks. password keyword, password encryption is enabled, but only the encrypted form appears there the password keyword, the passwords and other security-sensitive information in the aced in the output with the word "removed." -support commands are a compilation of several show commands and the output can be For a sample display of the output of the show tech-support command, see the individual d listed. e show tech-support command without arguments, the output displays the equivalent of mmands: 					

- 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 the "Usage Guidelines" section for more information.

Related Commands See the "Usage Guidelines" section.

show udld

To display the administrative and operational UDLD status, use the show udld command.

show udld interface-id

Syntax Description	interface-id	Name of the interface.
Defaults	This command	has no default settings.
Command Modes	Privileged EXE	C mode
Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(25)EW	Added support for the 10-Gigabit Ethernet interface.
Usage Guidelines	If you do not er interfaces is dis	nter an interface ID value, the administrative and operational UDLD status for all splayed.
Examples	This example s	hows how to display the UDLD state for Gigabit Ethernet interface 2/2:
	Switch# show w Interface Gi2,	udld gigabitethernet2/2 /2
	Port enable op Current bidird Current operat Message interv Time out inter No multiple ne Entry 1 Expiration Device ID Current ne Device nan Port ID: 2 Neighbor of Message in	rval: 5 eighbors detected n time: 146 : 1 eighbor state: Bidirectional me: 0050e2826000
	Switch#	

Related Commands	Command	Description		
	udld (global configuration mode)	Enables aggressive or normal mode in the UDLD protocol and sets the configurable message timer time.		
	udld (interface configuration mode)	Enables UDLD on an individual interface or prevents a fiber interface from being enabled by the udld (global configuration mode) command.		

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 vlan_id	(Optional) Displays information about a single VLAN identified by VLAN ID							
		number; valid values are from 1 to 4094.							
	name name	(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.							
	type	(Optional) Private VLAN type.							
efaults	This command	has no default settings.							
ommand Modes	Privileged EXE	C mode							
command History	Release	Modification							
Command history									
initiatia mistory	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.							
oniniana mistory	12.1(8a)EW 12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch. Added support for extended VLAN addresses.							
	12.1(12c)EW This example s								
	12.1(12c)EW This example si domain:	Added support for extended VLAN addresses.							
	12.1(12c)EW This example s	Added support for extended VLAN addresses. hows how to display the VLAN parameters for all VLANs within the administrative vlan Status Ports							
	12.1(12c)EW This example si domain: Switch# show	Added support for extended VLAN addresses. hows how to display the VLAN parameters for all VLANs within the administrative							
	12.1(12c)EW This example sidomain: Switch# show VLAN Name	Added support for extended VLAN addresses. hows how to display the VLAN parameters for all VLANs within the administrative vlan Status Ports							
	12.1(12c)EW This example sl domain: Switch# show VLAN Name 1 default	Added support for extended VLAN addresses. hows how to display the VLAN parameters for all VLANs within the administrative vlan Status Ports active Fa5/9							
	12.1(12c)EW This example sidomain: Switch# show VLAN Name 1 default 2 VLAN0002 3 VLAN003 4 VLAN004	Added support for extended VLAN addresses. hows how to display the VLAN parameters for all VLANs within the administrative vlan Status Ports							
	12.1(12c)EW This example sl domain: Switch# show VLAN Name 1 default 2 VLAN0002 3 VLAN0003 4 VLAN0004 5 VLAN0005	Added support for extended VLAN addresses. hows how to display the VLAN parameters for all VLANs within the administrative vlan Status Ports Active Fa5/9 Activ							
	12.1(12c)EW This example sidomain: Switch# show VLAN Name 1 default 2 VLAN0002 3 VLAN0003 4 VLAN0004 5 VLAN0005 6 VLAN0006	Added support for extended VLAN addresses. hows how to display the VLAN parameters for all VLANs within the administrative vlan Status Ports active Fa5/9							
Examples	12.1(12c)EW This example sl domain: Switch# show VLAN Name 1 default 2 VLAN0002 3 VLAN0003 4 VLAN0004 5 VLAN0005	Added support for extended VLAN addresses. hows how to display the VLAN parameters for all VLANs within the administrative vlan Status Ports Active Fa5/9 Activ							

Switch#

7

off

850 VLAN0850 917 VLAN0917 999 VLAN0999 1002 fddi-default 1003 trcrf-default 1004 fddinet-default 1005 trbrf-default					act: act: act: act: act:	ive ive ive ive	Fag Fag Fag Fag Fag Fag Fag	5/9 5/9 5/9 5/9 5/9			
VLAN	Туре	SAID	MTU	Parent	RingNo	Bridge	eNo	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
<(Dutput	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	AREHop	ps STEHops	Backup	CRF							
802	0	0	off								

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 Switch#	active	Fa5/9

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
        Trans1
        Trans2

        3
        enet
        100003
        1500
        -
        -
        -
        -
        -
        303
        0
```

Table 2-25 describes the fields in the show vlan command output.

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.			
Туре	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.			

Table 2-25 show vlan Command Output Fields

The following example shows how to verify that the primary vlan and secondary vlans are correctly associated with each other and the same association also exists on the PVLAN port:

Switch# show vlan private-vlan

Now, let's say that you remove the VLAN association, as follows:
You can use the following command to verify PVLAN configuration on the interface:

Switch#	show interface f3/2	status		
Port	Name	Status	Vlan Dup	lex Speed Type
Fa3/2		connected	pvlan seco a-fi	ull a-100 10/100BaseTX
Switch#	show interface f3/1	status		
Switch# Port	<pre>show interface f3/1 Name</pre>	status Status	Vlan Dupi	lex Speed Type
				lex Speed Type 111 a-100 10/100BaseTX

Related Commands Co

Command	Description
vlan (VLAN Database mode)	Configures a specific VLAN.
vlan database	Enters VLAN configuration mode.
vtp (global configuration mode)	Modifies the name of a VTP configuration storage file.

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	map-name	(Optional) Name of the VLAN access map.
Defaults	This command h	has no default settings.
ommand Modes	Privileged EXE	C mode
Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	This command s	shows how to display the contents of a VLAN access map:
xamples		
Examples		v lan access-map mordred up "mordred" 1
cxampies	Switch# show v Vlan access-map match:	up "mordred" 1 ip address 13
Examples	Switch# show v Vlan access-map match:	up "mordred" 1
Examples	Switch# show v Vlan access-maj match: action	up "mordred" 1 ip address 13
	Switch# show v Vlan access-maj match: action Switch#	ap "mordred" 1 ip address 13 a: forward capture Description

show vlan counters

To display the software-cached counter values, use the show vlan counters command.

show vlan [id vlanid] counters

Syntax Description	id vlanid	(Optional) Displays th	ne software-cached counter values for a specific VLAN.		
Defaults	This command has no default settings.				
Command Modes	Privileged EX	KEC mode			
Command History	Release 12.1(13)EW	Modification Support for this co	ommand was introduced on the Catalyst 4500 series switches.		
Usage Guidelines		he show vlan counters as for all VLANs are dis	command without specifying the VLAN ID, the software-cached played.		
Examples	Switch# show	shows how to display the shows how to display the shows how to display the shows the s	the software-cached counter values for a specific VLAN:		
	Vlan Id L2 Unicast H L2 Unicast O L3 Input Uni L3 Input Uni L3 Output Un L3 Output Un L3 Output Mu L3 Output Mu L3 Input Mu	Packets Detets Least Packets Least Octets Licast Packets Licast Octets Licast Packets Licast Octets Licast Octets Licast Octets Licast Octets	: 1 : 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0		
Related Commands	Command		Description		
	clear vlan co	ounters	Clears the software-cached counter values to start from zero again for a specified VLAN or all existing VLANs.		

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

 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

Related Commands	Command	Description
	switchport mode	Sets the interface type.
	vlan (global configuration) (refer to Cisco IOS documentation)	Enters global VLAN configuration mode.
	vlan (VLAN configuration) (refer to Cisco IOS documentation)	Enters VLAN configuration mode.

show vlan internal usage

To display information about the internal VLAN allocation, use the show vlan internal usage command.

show vlan [id vlan-id] internal usage

Syntax Description Defaults Command Modes	id <i>vlan-id</i> This command Privileged EXE	valid values are from	
Command History	Release 12.1(19)EW	Modification Support for this cor	nmand was introduced on the Catalyst 4500 series switch.
Examples	-	nnel6 chernet1/2	formation about the current internal VLAN allocation:
	VLAN:		formation about the internal VLAN allocation for a specific
	1030 GigabitEt		
Related Commands	Command vlan internal a	allocation policy	Description Configures the internal VLAN allocation scheme.

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	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 con	nmand was intro	duced 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			e show vlan mt	u command:		
	Switch# show		MaxMTU(port)	MTU_Mismatch		
	1 1500 Switch>	1500	1500	 No		
Related Commands	Command		Descripti	on		
	mtu		•	umbo frames on an interface by adjusting the a size of a packet or maximum transmission unit		

show vlan private-vlan

To display private VLAN information, use the show vlan private-vlan command.

show vlan private-vlan [type]

Syntax Description	type		ptional) Displays th mmunity, nonopera	e private VLAN type; valid types are isolated, primary, tional, and normal.
Defaults	This con	nmand has 1	no default settings.	
Command Modes	Privilege	ed EXEC m	ode	
Command History	Release	N	Aodification	
	12.1(8a)	EW S	upport for this com	mand was introduced on the Catalyst 4500 series switch.
	12.2(20))EW S	Support for commun	ity VLAN was added.
Usage Guidelines	regular V indicates	VLAN has b s that two V	been used in the priv LANs have been as	command displays a VLAN type as normal, it indicates tha rate VLAN configuration. When normal is displayed, this sociated before the type was set, and the private VLAN is no for debugging purposes.
-	regular V indicates operation	VLAN has b s that two V nal. This inf	been used in the priv LANs have been as formation is useful t	vate VLAN configuration. When normal is displayed, this sociated before the type was set, and the private VLAN is no for debugging purposes.
-	regular V indicates operation This exa	VLAN has b s that two V nal. This inf mple shows	Deen used in the priv LANs have been as formation is useful to be how to display info	vate VLAN configuration. When normal is displayed, this sociated before the type was set, and the private VLAN is no
	regular V indicates operation This exa Switch#	VLAN has b s that two V nal. This inf mple shows	been used in the priv LANs have been as formation is useful to how to display info private-vlan	vate VLAN configuration. When normal is displayed, this sociated before the type was set, and the private VLAN is no for debugging purposes.
	regular V indicates operation This exa Switch#	VLAN has b s that two V nal. This inf mple shows show vlan Secondary 301 302	Type community community	vate VLAN configuration. When normal is displayed, this sociated before the type was set, and the private VLAN is no for debugging purposes.
	regular V indicates operation This exa Switch# Primary 2	VLAN has b s that two V nal. This inf mple shows show vlan Secondary 301	heen used in the priv LANs have been as formation is useful the how to display infor private-vlan Type community	vate VLAN configuration. When normal is displayed, this sociated before the type was set, and the private VLAN is no for debugging purposes.
	regular V indicates operation This exa Switch# Primary 2 2	VLAN has b s that two V nal. This inf mple shows show vlan Secondary 301 302 10	Type community community community	vate VLAN configuration. When normal is displayed, this sociated before the type was set, and the private VLAN is no for debugging purposes.
Usage Guidelines	regular V indicates operation This exa Switch# Primary 2 2 100	VLAN has b s that two V nal. This inf mple shows show vlan Secondary 301 302 10 101 151 202	een used in the priv LANs have been as formation is useful to show to display infor private-vlan Type 	vate VLAN configuration. When normal is displayed, this sociated before the type was set, and the private VLAN is no for debugging purposes.

This example shows how to display information about all currently configured private VLAN types:

Switch# show vlan private-vlan type

```
Vlan Type

202 primary

303 community

304 community

305 community

306 community

307 community

308 normal

309 community

440 isolated

Switch#
```

Table 2-26 describes the fields in the show vlan private-vlan command output.

Field	Description
Primary	Number of the primary VLAN.
Secondary	Number of the secondary VLAN.
Secondary-Type	Secondary VLAN type is isolated or community.
Ports	Indicates the ports within a VLAN.
Туре	Type of VLAN; possible values are primary, isolated , community, nonoperational, or normal .

Table 2-26show vlan private-vlan Command Output Fields

Related Commands

Command	Description
private-vlan	Configures private VLANs and the association between a private VLAN and a secondary VLAN.
private-vlan mapping	Creates a mapping between the primary and the secondary VLANs so that both share the same primary VLAN SVI.

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 mode

Command HistoryReleaseModification12.1(12)EWThis command was introduced on the Catalyst 4500 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	Command	Description
	remote-span	Converts a VLAN into an RSPAN VLAN.
	vlan (VLAN Database mode)	Configures a specific VLAN.

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			
	VQPQueries:0VQPResponses:0VMPSChanges:0VQPShutdowns:0VQPDenied:0VQPWrong Domain:0VQPWrong Version:0VQPInsufficient Resource:0Switch#			

Related Commands	Command	Description
	vmps reconfirm (privileged EXEC)	Sends VLAN Query Protocol (VQP) queries to reconfirm all the dynamic VLAN assignments with the VLAN Membership Policy Server (VMPS).

show vtp

To display VTP statistics and domain information, use the show vtp command.

show vtp {counters | status}

Cuntou Deseriation				
Syntax Description	counters	Specifies the VTP		
	status	Specifies the VTP	domain status.	
Defaults	This comman	id has no default sett	ings.	
Command Modes	Privileged EX	XEC mode		
Command History	Release	Modification		
	12.1(8a)EW	Support for thi	is command was introd	luced on the Catalyst 4500 series switch.
Examples	This example	shows how to displa	ay the VTP statistics:	
	VTP statist Summary adver Subset adver Request adver Submary adver Subset adver Request adver Number of co	ertisements receive ertisements receive ertisements receive ertisements transmi ertisements transmi onfig revision erro onfig digest errors statistics:	d : 1 ed : 0 itted : 31 tted : 1 itted : 0 ors : 0	Summary advts received from non-pruning-capable device
	Fa5/9 Switch#	1555	1564	0
	Switch# show VTP Version Configuration Maximum VLAN	w vtp status on Revision Ns supported local disting VLANs ng Mode Name Mode	ay the VTP domain sta : 2 : 250 ly : 1005 : 33 : Server : Lab_Network : Enabled : Enabled : Disabled	itus:

```
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 interfac
e 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#
```

Table 2-27 describes the fields in the show vtp command output.

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.

Table 2-27show vtp Command Output Fields

Related	Commands	(

nands	Command	Description
	vtp (global configuration mode)	Modifies the name of a VTP configuration storage file.
	vtp client	Places a device in VTP client mode.
	vtp domain	Configures the administrative domain name for a device.
	vtp password	Creates a VTP domain password.
	vtp pruning	Enables pruning in the VLAN database.
	vtp server	Places the device in VTP server mode.
	vtp transparent	Places device in VTP transparent mode.
	vtp v2-mode	Enables version 2 mode.

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 Catalyst 4500 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.

Γ

Related Commands	Command	Description
	snmp ifindex persist	Enables ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) on a specific interface.
	snmp-server ifindex persist	Enables ifIndex values that will remain constant across reboots for use by SNMP.

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. To disable ifIndex persistence only on a specific interface, use the **no** form of this command.

snmp ifindex persist

no snmp ifindex persist

Syntax Description	This command has no arguments or keywords.			
Defaults	Disabled.	Disabled.		
Command Modes	Interface configuration mode			
Command History	Release	Modification		
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 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 sh	nows 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)	<pre># snmp-server ifindex persist # interface fastethernet 1/1 iif)# no snmp ifindex persist iif)# exit</pre>		

Related Commands	Command	Description
	snmp ifindex clear	Clears any previously configured snmp ifindex commands that were entered for a specific interface.
	snmp ifindex persist	Enables ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) on a specific interface.

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 | stpx | vlancreate | vlandelete | vtp] [mac-notification [change | move | threshold]

no snmp-server enable traps [flash [insertion | removal] | fru-ctrl | port-security [trap-rate *trap-rate*] | **removal | stpx | vlancreate | vlandelete | vtp] [mac-notification**]

Syntax Description	flash	(Optional) Controls the SNMP FLASH trap notifications.
ymax Deseription		
	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 trap-rate	(Optional) Sets the number of traps per second.
	stpx	(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.
	mac-notification	(Optional) Controls the SNMP MAC trap notifications.
	change	(Optional) Controls the SNMP MAC change trap notifications
	move	(Optional) Controls the SNMP MAC move trap notifications
	threshold	(Optional) Controls the SNMP MAC threshold trap notifications
efaults	SNMP notifications are	e disabled.
Command Modes	Global configuration m	

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(31)SG	Support for MAC notification was added.

Usage Guidelines If yo

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.

This list of the MIBs is 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.
- **stpx**—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 is 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)#
```

This example shows how to enable the MAC address change MIB notification:

Switch(config)# snmp-server enable traps mac-notification change Switch(config)#

SNMP traps can be enabled with a rate-limit to detect port-security violations due to restrict mode. The following example shows how to enable traps for port-security with a rate of 5 traps per second:

Switch(config)# snmp-server enable traps port-security trap-rate 5
Switch(config)#

Related Commands	Command	Description	
	clear mac-address-table dynamic	Clears the dynamic address entries from the Layer 2 MAC address table.	
	mac-address-table notification	Enables MAC address notification on a switch.	
	show mac-address-table notification	Displays the MAC address table notification status and history.	
	snmp-server enable traps	Enables SNMP notifications.	
	snmp trap mac-notification change	Enables SNMP MAC address notifications.	

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. To globally disable inIndex persistence, use the **no** form of this command.

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 Catalyst 4500 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 the 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	Command	Description
	snmp ifindex clear	Clears any previously configured snmp ifindex commands that were entered for a specific interface.
	snmp ifindex persist	Enables ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) on a specific interface.

snmp-server ifindex persist compress

To configure the format of the ifIndex table in a compressed format, use the **snmp-server ifindex persist compress** command. To place the table in a decompressed format, use the **no** form of this command.

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(46)SG
 Support for this command was introduced on the Catalyst 4500 series switches.

Usage Guidelines This command is hidden on Supervisor Engine V and later supervisor engines because the ifIndex table is always in a compressed format on those supervisor engines.

At bootup, if the nvram:ifIndex-table.gz file (the ifIndex table ina 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

outer(config)# simp-server fillindex persist compress

This example shows how to disable compression of the ifIndex table:

Router(config)# no snmp-server ifindex persist compress

Related Commands	Command	Description
	snmp ifindex clear	Clears any previously configured snmp ifindex commands that were entered for a specific interface.
	snmp ifindex persist	Enables ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) on a specific interface.
	snmp-server ifindex persist	Enables ifIndex values that will remain constant across reboots for use by SNMP.

snmp trap mac-notification change

To enable SNMP MAC address notifications, use the **snmp trap mac-notification** command. To return to the default setting, use the **no** form of this command.

snmp trap mac-notification change {added | removed}

no snmp trap mac-notification change {added | removed}

Syntax Description	added	*	ling the MAC address notification trap whenever a MAC ed to an interface.
	removed	-	ling the MAC address notification trap whenever a MAC oved from an interface.
Defaults	MAC address additi	on and removal are d	isabled.
Command Modes	Interface configuration mode		
Command History	Release	Modification	
-	12.2(31)SG	Support for this con	nmand was introduced on the Catalyst 4500 series switch.
Usage Guidelines	snmp trap mac-not	ification change con e traps mac-notifica	ication trap for a specific interface by using the nmand, the trap is generated only when you enable the tion change and the mac address-table notification change
-	snmp trap mac-not snmp-server enable global configuration	ification change con e traps mac-notifica commands.	nmand, the trap is generated only when you enable the tion change and the mac address-table notification change
Usage Guidelines Examples	snmp trap mac-not snmp-server enable global configuration This example shows Switch(config)# ir	ification change con e traps mac-notifica commands. how to enable the M nterface gigabiteth	nmand, the trap is generated only when you enable the tion change and the mac address-table notification change IAC notification trap when a MAC address is added to a port
	snmp trap mac-not snmp-server enable global configuration This example shows Switch(config)# ir Switch(config-if)#	ification change come traps mac-notificate commands. how to enable the Materface gigabiteth snmp trap mac-not settings by entering	nmand, the trap is generated only when you enable the tion change and the mac address-table notification change IAC notification trap when a MAC address is added to a port hernet1/1
Examples	snmp trap mac-not snmp-server enable global configuration This example shows Switch(config)# ir Switch(config)if You can verify your	ification change come traps mac-notificate commands. how to enable the Materface gigabiteth snmp trap mac-not settings by entering	nmand, the trap is generated only when you enable the tion change and the mac address-table notification change AC notification trap when a MAC address is added to a port ternet1/1 dification change added
Examples	snmp trap mac-not snmp-server enable global configuration This example shows Switch(config)# ir Switch(config)if) You can verify your privileged EXEC co	ification change come traps mac-notification commands. how to enable the Materface gigabiteth snmp trap mac-not settings by entering mmand.	nmand, the trap is generated only when you enable the tion change and the mac address-table notification change [AC notification trap when a MAC address is added to a port: hernet1/1 dification change added the show mac address-table notification change interface
	snmp trap mac-not snmp-server enable global configuration This example shows Switch(config)# in Switch(config-if)# You can verify your privileged EXEC co	ification change come traps mac-notification commands. how to enable the Materface gigabiteth snmp trap mac-not settings by entering mmand.	IAC notification trap when a MAC address is added to a port mernet1/1 deres
Examples	snmp trap mac-not snmp-server enable global configuration This example shows Switch(config)# ir Switch(config-if)# You can verify your privileged EXEC co Command clear mac-address	ification change come e traps mac-notifica commands. how to enable the Materface gigabiteth snmp trap mac-not settings by entering mmand.	nmand, the trap is generated only when you enable the tion change and the mac address-table notification change IAC notification trap when a MAC address is added to a port: ternet1/1 Sification change added the show mac address-table notification change interface Description Clears the address entries from the Layer 2 MAC address table.

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 this 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 mode

 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 4506 series 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	Command	Description	
	spanning-tree cost	Calculates the path cost of STP on an interface.	
	spanning-tree portfast default	Enables PortFast by default on all access ports.	
	spanning-tree portfast (interface configuration mode)	Enables PortFast mode.	
	spanning-tree port-priority	Prioritizes an interface when two bridges compete for position as the root bridge.	
	spanning-tree uplinkfast	Enables the UplinkFast feature.	
	spanning-tree vlan	Configures STP on a per-VLAN basis.	
	show spanning-tree	Displays spanning-tree information.	

spanning-tree bpdufilter

To enable BPDU filtering on an interface, use the **spanning-tree bpdufilter** command. To return to the default settings, use the **no** form of this command.

spanning-tree bpdufilter {enable | disable}

no spanning-tree bpdufilter

Syntax Description	enable	Enables BPDU filtering on this interface.
eynax booonprion	disable	Disables BPDU filtering on this interface.
Defaults	Disabled	
Command Modes	Interface config	guration mode
Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Usage Guidelines		
Caution	interface is app	entering the spanning-tree bpdufilter enable command. Enabling BPDU filtering on an proximately equivalent to disabling the spanning tree for this interface. It is possible to loops if this command is not correctly used.
	-	ing Layer 2 protocol tunneling on all the service provider edge switches, you must enable BPDU filtering on the 802.1Q tunnel ports by entering the spanning-tree bpdufilter nd.
		allows you to prevent a port from sending and receiving BPDUs. The configuration is he whole interface, whether it is trunking or not. This command has three states:
	• spanning-1 the interfac	tree bpdufilter enable—This state unconditionally enables the BPDU filter feature on ce.
	• spanning-1 the interfac	tree bpdufilter disable—This state unconditionally disables the BPDU filter feature on ce.
	interface is	ng-tree bpdufilter —This state enables the BPDU filter feature on the interface if the in operational PortFast state and if the spanning-tree portfast bpdufilter default is configured.

Examples This example shows how to enable the BPDU filter feature on this interface: Switch(config-if)# spanning-tree bpdufilter enable Switch(config-if)#

Related Commands	Command	Description
	show spanning-tree	Displays spanning-tree information.
	spanning-tree portfast bpdufilter default	Enables the BPDU filtering by default on all PortFast ports.

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	
Command Modes	Interface config	uration mode
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	Command	Description
	show spanning	Displays spanning-tree information.
	spanning-tree default	portfast bpdufilter Enables the BPDU filtering by default on all PortFast ports.

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	<i>cost</i> 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 mode		
Command History	Release Modification		
	12.1(8a)EWSupport for this composition	mmand was introduced on the Catalyst 4500 series switch	
Examples			
	<pre>Switch(config-if)# spanning-tree Switch(config-if)#</pre>	cost 250	
Related Commands	Command	Description	
	spanning-tree portfast default	Enables PortFast by default on all access ports.	
	spanning-tree portfast (interface configuration mode)	Enables PortFast mode.	
	spanning-tree port-priority	Prioritizes an interface when two bridges compete for position as the root bridge.	
	spanning-tree uplinkfast	Enables the UplinkFast feature.	
	spanning-tree vlan	Configures STP on a per-VLAN basis.	
	show spanning-tree	Displays spanning-tree information.	

Γ

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 mode

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 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 verify 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	Command	Description
	show etherchannel	Displays EtherChannel information for a channel.
	show interfaces status	Displays the interface status or a list of interfaces in error-disabled state.
	shutdown (refer to Cisco IOS documentation)	Disables a port.

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 mode

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

2-681

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	loop Ena	bles the loop guard mode on the interface.
	root Ena	bles root guard mode on the interface.
	none Set	s the guard mode to none.
Defaults	Root guard is di	sabled.
Command Modes	Interface config	uration mode
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		Loop guard support was added.
Examples	This example sh	nows how to enable root guard: if)# spanning-tree guard root
Examples Related Commands	This example sh Switch(config-	nows how to enable root guard: if)# spanning-tree guard root

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	Specifies that the interface is a point-to-point link.	
	shared	Specifies that the interface is a shared medium.	
Defaults	Link type is deriv	ed from the duplex mode.	
Command Modes	Interface configuration mode		
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 works only 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.		
	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	Command	Description	
	show spanning-t	ree Displays spanning-tree information.	

Displays spanning-tree information.

2-683

spanning-tree loopguard default

show spanning-tree

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 mode	
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 por from becoming the designated port because of a failure leading to a unidirectional link. Loop guard operates only on ports that are considered point-to-point by the spanning tree. Individual loop-guard port configuration overrides this global default.	
Examples	This example sh	ows how to enable loop guard:
	Switch(config)# spanning-tree loopguard default Switch(config)#	
Related Commands	Command	Description
	spanning-tree g	guard Enables root 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			
	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.	
<u>Z1</u> Caution	 Be careful when using the spanning-tree mode command to switch between PVST+ and MST mode 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	Command	Description	

spanning-tree mst

To set the path cost and port-priority parameters for any MST instance (including the CIST with instance ID 0), 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**}

Cuntary Description		
Syntax Description	instance-id	Instance ID number; valid values are from 0 to 15.
	cost cost	(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 configurat	tion mode
Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
Usage Guidelines		<i>t</i> values indicate higher costs. When entering the <i>cost</i> value, do not include a comma imple, enter 1000 , not 1,000 .
Usage Guidelines	in the entry; for exa	<i>t</i> values indicate higher costs. When entering the <i>cost</i> value, do not include a comma imple, enter 1000 , not 1,000 . iority <i>prio</i> values indicate smaller priorities.
Usage Guidelines	in the entry; for exa The higher port-pr	imple, enter 1000 , not 1,000 . iority <i>prio</i> values indicate smaller priorities. depends on the port speed; faster interface speeds indicate smaller costs. MST
	in the entry; for exa The higher port-pr By default, the cost always uses long pa	imple, enter 1000 , not 1,000 . iority <i>prio</i> values indicate smaller priorities. depends on the port speed; faster interface speeds indicate smaller costs. MST
	in the entry; for exa The higher port-pr By default, the cost always uses long pa This example shows	<pre>imple, enter 1000, not 1,000. iority prio values indicate smaller priorities. depends on the port speed; faster interface speeds indicate smaller costs. MST ath costs. s how to set the interface path cost: # spanning-tree mst 0 cost 17031970</pre>
Usage Guidelines Examples	in the entry; for exa The higher port-pr By default, the cost always uses long pa This example shows Switch(config-if) Switch(config-if)	<pre>imple, enter 1000, not 1,000. iority prio values indicate smaller priorities. depends on the port speed; faster interface speeds indicate smaller costs. MST ath costs. s how to set the interface path cost: # spanning-tree mst 0 cost 17031970</pre>

Related Commands	Command	Description
	show spanning-tree mst	Displays MST protocol information.
	spanning-tree port-priority	Enables an interface when two bridges compete for position as the root bridge.
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	s no arguments or keywords.		
Defaults	The default setting	gs are as follows:		
	No VLANs are mapped to any MST instance.All VLANs are mapped to the CIST instance.			
	• The region na	me is an empty string.		
	• The revision r	number is 0.		
Command Modes	Global configurati	on mode		
Command History	Release	Modification		
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.		
Usage Guidelines	The MST configu	ration consists of three main parameters:		
	Instance VLA	N 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 the secondary VLANs to the same instance as the associated primary VLAN, when you exit the MST configuration submode, a message displays and lists the secondary VLANs that are not mapped to the same instance as the associated primary VLAN. The message is as follows:			
	These secondary ->3	vlans are not mapped to the same instance as their primary:		
	The abort comma	nd 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 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	Command	DescriptionMaps a VLAN or a set of VLANs to an MST instance.	
	instance		
	name	Sets the MST region name.	
	revision	Sets the MST configuration revision number.	
	show spanning-tree mst	Displays MST protocol information.	

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 this 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 Catalyst 4500 series switch; valid values are from 4 to 30 seconds.		
Defaults	The forward dela	y timer is set for 15 seconds.	
Command Modes	Global configura	ion mode	
Command History	Release	Modification	
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.	
Examples	This example sho	ws how to set the forward-delay timer:	
	Switch(config)# Switch(config)#	spanning-tree mst forward-time 20	
Related Commands	Command	Description	
		ree mst Displays MST protocol information.	

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 this command.

spanning-tree mst hello-time seconds

no spanning-tree mst hello-time

Syntax Description	seconds	Number of seconds to set the hello-time delay timer for all the instances on the Catalyst 4500 series switch; valid values are from 1 to 10 seconds.	
Defaults	The hello-time	delay timer is set for 2 seconds.	
Command Modes	Global configur	ration mode	
Command History	Release	Modification	
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.	
Jsage Guidelines	If you do not sp	becify the <i>hello-time</i> value, the value is calculated from the network diameter.	
xamples	This example shows how to set the hello-time delay timer:		
	Switch(config) Switch(config)	# spanning-tree mst hello-time 3 #	
Related Commands	Command	Description	
	show spanning	tree mst Displays MST protocol information.	

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 this 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 Catalyst 4500 series switch; valid values are from 6 to 40 seconds.		
Defaults	The max-age tin	er is set for 20 seconds.	
Command Modes	Global configur	tion mode	
Command History	Release	Modification	
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switc	:h
Examples	This example sl	ows how to set the max-age timer:	
	Switch(config) Switch(config)	spanning-tree mst max-age 40	
Related Commands	Command	Description	
	show spanning	tree mst Displays MST protocol information.	-

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 this command.

spanning-tree mst max-hops hopnumber

no spanning-tree mst max-hops

Syntax Description	hopnumber	Number of possible hops in the region before a BPDU is discarded; valid values are from 1 to 40 hops.
Defaults	Number of hop	s is 20.
Command Modes	Global configu	ration mode
Command History	Release 12.1(12c)EW	Modification Support for this command was introduced on the Catalyst 4500 series switch
Examples	-	hows how to set the number of possible hops in the region before a BPDU is discarded to 25) # spanning-tree mst max-hops 25
Related Commands	Switch(config) # Description
	show spanning	-

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 this command.

spanning-tree mst instance-id root {primary | secondary} | {priority prio} [diameter dia
 [hello-time hello]]

no spanning-tree mst root

Syntax Description	instance-id	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 prio	Sets the bridge priority; see the "Usage Guidelines" section for valid values and additional information.
	diameter dia	(Optional) Sets the timer values for the bridge based on the network diameter; valid values are from 2 to 7.
	hello-time hello	(Optional) Specifies the duration between the generation of configuration messages by the root switch.
	Bridge priority is a Global configurati	
Command Modes	Global configurati	ion mode
Defaults Command Modes Command History	Global configurati	ion mode Modification
Command Modes Command History	Global configurati Release 12.1(12c)EW	ion mode Modification Support for this command was introduced on the Catalyst 4500 series switch
Command Modes Command History	Global configurati Release 12.1(12c)EW The bridge priority	ion mode Modification Support for this command was introduced on the Catalyst 4500 series switch
Command Modes Command History	Global configurati Release 12.1(12c)EW The bridge priority 4096, 8192, 12288 and 61440.	ion mode Modification Support for this command was introduced on the Catalyst 4500 series switch y can be set in increments of 4096 only. When you set the priority, valid values are 0,
Command Modes Command History	Global configurati Release 12.1(12c)EW The bridge priority 4096, 8192, 12288 and 61440. You can set the priority	Modification Support for this command was introduced on the Catalyst 4500 series switch y can be set in increments of 4096 only. When you set the priority, valid values are 0, 3, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344,
Command Modes	Global configurati Release 12.1(12c)EW The bridge priority 4096, 8192, 12288 and 61440. You can set the priority The spanning-tree	Modification Support for this command was introduced on the Catalyst 4500 series switch y can be set in increments of 4096 only. When you set the priority, valid values are 0, 3, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, iority to 0 to make the switch root.

Displays MST protocol information.

Related Commands	Command	Description		
		panning-tree mst 0 root primary diameter 7 hello-time 2 panning-tree mst 5 root primary		
Examples	This example shows how to set the priority and timer values for the bridge:			

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 Sp	ecifies 32-bit-based values for port path costs.			
	short Specifies 16-bit-based values for port path costs.				
Defaults	Port path cost h	nas 32-bit-based values.			
Command Modes	Global configu	ration mode			
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	Command				
neiateo commaños		Description Displays spanning-tree state information			
	show spanning	g-tree Displays spanning-tree state information.			

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	nk Enables PortFast on the interface even while in the trunk mode.			
Defaults	PortFast mo	ode is disabled.			
Command Modes	Interface co	onfiguration mode			
Command History	Release	Modification			
	12.1(8a)EV	V Support for this command was introduced on the Catalyst 4500 series switch			
	12.1(12c)E	W The disable and trunk options were added.			
Usage Guidelines		use this feature only with interfaces that connect to end stations; otherwise, an accidental op could cause a data packet loop and disrupt the Catalyst 4500 series switch and network			
	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.				
	• spanni	ng-tree portfast trunk —This command allows you to configure PortFast on trunk ports.			
	•	ou enter the spanning-tree portfast trunk command, the port is configured for PortFast n 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	Command	Description	
	spanning-tree cost	Calculates the path cost of STP on an interface.	
	spanning-tree portfast default	Enables PortFast by default on all access ports.	
	spanning-tree port-priority	Prioritizes an interface when two bridges compete for position as the root bridge.	
	spanning-tree uplinkfast	Enables the UplinkFast feature.	
	spanning-tree vlan	Configures STP on a per-VLAN basis.	
	show spanning-tree	Displays spanning-tree state information.	

spanning-tree portfast bpdufilter default

To enable the BPDU filtering by default on all PortFast ports, use the **spanning-tree portfast bpdufilter default** command. To return to the default settings, use the **no** form of this command.

spanning-tree portfast bpdufilter default

no spanning-tree portfast bpdufilter default

- **Syntax Description** This command has no keywords or arguments.
- **Defaults** BPDU filtering is disabled.
- **Command Modes** Global configuration mode

 Release
 Modification

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

Usage Guidelines

The **spanning-tree portfast bpdufilter default** command enables BPDU filtering globally on the Catalyst 4500 series switch. BPDU filtering prevents a port from sending or receiving any BPDUs.

You can override the effects of the **spanning-tree portfast bpdufilter default** command by configuring BPDU filtering at the interface level.

<u>Note</u>

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 Catalyst 4500 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 bpdufilter default
Switch(config)#

Related Commands	Command	Description	
	show spanning-tree mst	Displays MST protocol information.	
spanning-tree bpdufilter		Enables BPDU filtering on an interface.	

spanning-tree portfast bpduguard default

To enable BPDU guard by default on all the 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 mode

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 the interfaces that connect to the end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt the Catalyst 4500 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	Command	Description	
	show spanning-tree mst	Displays MST protocol information.	
spanning-tree bpduguard		Enables BPDU guard on an interface.	

spanning-tree portfast default

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.

	no spanning-	tree portfast defaul	t	
Syntax Description	This command has	s no arguments or ke	ywords.	
Defaults	PortFast is disable	PortFast is disabled.		
Command Modes	Global configuration mode			
Command History	Release	Modification		
••••••••	12.1(12c)EW		ommand was introduced on the Catalyst 4500 series switch.	
Usage Guidelines	to end stations; of Catalyst 4500 seri An interface with linkup occurs with	nerwise, an accidenta es switch and networ PortFast mode enabl rout waiting for the s ortFast mode on indiv	You should use this command only with the interfaces that connect al topology loop could cause a data packet loop and disrupt the ek operation. The dis moved directly to the spanning-tree forwarding state when tandard forward-time delay. Tridual interfaces using the spanning-tree portfast (interface	
Examples	This example show	ws how to globally en	nable PortFast by default on all access ports:	
	Switch(config)# Switch(config)#	spanning-tree port	fast default	
Related Commands	Command		Description	
	show spanning-ti	·ee	Displays spanning-tree state information.	
	spanning-tree po configuration mo		Enables PortFast 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; valic	I values are from 0 to 240 in increments of 16.
Defaults	Port priority val	ue is set to 128.	
Command Modes	Interface config	uration mode	
Command History	Release	Modification	
	12.1(8a)EW	Support for this com	mand was introduced on the Catalyst 4500 series switch.
Examples			e possibility that the spanning-tree instance 20 will be chosen as et 2/1:
Examples	the root-bridge of	on interface FastEtherno	et 2/1:
	the root-bridge of Switch (config-	on interface FastEtherno	et 2/1:
	the root-bridge of Switch(config- Switch(config-	on interface FastEtherno if)# spanning-tree p if)#	et 2/1: prt-priority 0
	the root-bridge of Switch(config- Switch(config- Command spanning-tree	on interface FastEtherno if)# spanning-tree p if)#	Description
	the root-bridge of Switch(config- Switch(config- Command spanning-tree spanning-tree	on interface FastEtherno if)# spanning-tree po if)# cost portfast default portfast (interface	Description Calculates the path cost of STP on an interface.
	the root-bridge of Switch(config- Switch(config- Command spanning-tree spanning-tree spanning-tree	on interface FastEtherno if)# spanning-tree po if)# cost portfast default portfast (interface mode)	Description Calculates the path cost of STP on an interface. Enables PortFast by default on all access ports.
Examples Related Commands	the root-bridge of Switch (config- Switch (config- Command spanning-tree spanning-tree spanning-tree configuration	on interface FastEtherno if)# spanning-tree po if)# cost portfast default portfast (interface mode) uplinkfast	Description Calculates the path cost of STP on an interface. Enables PortFast by default on all access ports. Enables PortFast mode.

spanning-tree uplinkfast

To enable the UplinkFast feature, use the **spanning-tree uplinkfast** command. To disable UplinkFast, use the **no** form of this command.

spanning-tree uplinkfast [max-update-rate packets-per-second]

no spanning-tree uplinkfast [max-update-rate]

Syntax Description	max-update-rate packets_per_second	(Optional) Specifies the maximum rate (in packets per second) at which update packets are sent; valid values are from 0 to 65535.
Defaults	The default settings anDisabled.Maximum update	
Command Modes	Global configuration 1	node
Command History	Release Mo	dification
-	12.1(8a)EW Suj	oport for this command was introduced on the Catalyst 4500 series switch
Usage Guidelines	When UplinkFast is co selected as root. All ir	be used only on access switches. onfigured, the bridge priority is changed to 49,152 so that this switch will not be iterface path costs of all spanning-tree interfaces belonging to the specified as are also increased by 3000.
	switchover to an altern state. During this time topology change, a mu	etects that the root interface has failed, the UplinkFast feature causes an immediate nate root interface, transitioning the new root interface directly to the forwarding , a topology change notification is sent. To minimize the disruption caused by the alticast packet is sent to 01-00-0C-CD-CD for each station address in the ept for those associated with the old root interface.
	enabled) and change t	e uplinkfast max-update-rate command to enable UplinkFast (if not already he rate at which the update packets are sent. Use the no form of this command to of 150 packets per second.
Examples	Switch(config)# spa	ow to enable UplinkFast and set the maximum rate to 200 packets per second: nning-tree uplinkfast nning-tree uplinkfast max-update-rate 200

Related Commands	Co	0
------------------	----	---

ed Commands	Command	Description	
	spanning-tree cost	Calculates the path cost of STP on an interface.	
	spanning-tree port-priority	Prioritizes an interface when two bridges compete for position as the root bridge.	
	spanning-tree portfast default	Enables PortFast by default on all access ports.	
	spanning-tree portfast (interface configuration mode)	Enables PortFast mode.	
	spanning-tree vlan	Configures STP on a per-VLAN basis.	

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	vlan_id	VLAN identification number; valid values are from 1 to 4094.			
	forward-time second	<i>ds</i> (Optional) Sets the STP forward delay time; valid values are from 4 to 30 seconds.			
	hello-time seconds	(Optional) Specifies, in seconds, the time between configuration messages generated by the root switch; valid values are from 1 to 10 seconds.			
	max-age seconds	(Optional) Sets the maximum time, in seconds, that the information in a BPDU is valid; valid values are from 6 to 40 seconds.			
	priority priority	(Optional) Sets the STP bridge priority; valid values are from 0 to 65535.			
	protocol protocol	(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 net-diamet	<i>er</i> (Optional) Specifies the maximum number of bridges between two end stations; valid values are from 2 to 7.			
Defaults	The default settings a • Forward-time—1				
	 Hello-time—2 se 				
	 Max-age—20 sec 				
	 Priority—32768 with STP enabled; 128 with MST enabled 				
	Root—No STP root				
Command Modes	Global configuration	mode			
Command History	Release M	odification			
communa motory		pport for this command was introduced on the Catalyst 4500 series switch.			
		pport for extended addressing was added.			
		11			

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)#

Relat

ated Commands	Command	Description		
	spanning-tree cost	Calculates the path cost of STP on an interface. Prioritizes an interface when two bridges compete for position as the root bridge.		
	spanning-tree port-priority			
	spanning-tree portfast default	Enables PortFast by default on all access ports.		
	spanning-tree portfast (interface configuration mode)	Enables PortFast mode.		
	spanning-tree vlan	Configures STP on a per-VLAN basis.		
	show spanning-tree	Displays spanning-tree state information.		

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 [10 | 100 | 1000] | nonegotiate}

no speed

Syntax Description	ion10(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 [10 100 (Optional) Enables the interface to autonegotiate the speed and specify the exact	
	1000]	values to advertise when autonegotiating.
	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 [10 100]]	Auto
100-Mbps fiber modules	Not applicable	Not applicable
Gigabit Ethernet Interface	speed nonegotiate	Nonegotiate
10/100/1000	speed [10 100 1000 auto [10 100 1000]]	Auto
1000	Not applicable	Not applicable

Command Modes Interface configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch
12.2(20)EWA	Support for auto negotiating specific speeds added.

Usage Guidelines Table 2-28 lists the supported command options by interface.

Interface Type	Supported Syntax	Default Setting	Guidelines
10/100-Mbps module	speed [10 100 auto]	auto	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 10 or 100 and you do not configure the duplex setting, the duplex is set to half.
			If the speed is set to 1000 or auto with any subset containing 1000 (e.g. speed auto 10 1000 or speed auto on a 10/100/1000 port), you will not able to set half duplex.
1000	Not applicable.	Not applicable.	The speed is always 1000.
			The duplex is half.

 Table 2-28
 Supported speed Command Options

If you configure the interface speed and duplex commands manually and enter a value other than **speed auto** (for example, 10 or 100 Mbps), make 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.



Catalyst 45006 switches cannot automatically negotiate the interface speed and the duplex mode if either connecting interface is configured to a value other than **auto**.



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

Table 2-29 describes the system's performance for different combinations of the duplex and speed modes. The specified **duplex** command that is configured with the specified **speed** command produces the resulting system action.

duplex Command	speed Command	Resulting System Action
duplex auto	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

Table 2-29 System Action Using duplex and speed Commands

Examples

This example shows how to set the interface speed to 100 Mbps on the Fast Ethernet interface 5/4:

Switch(config)# interface fastethernet 5/4
Switch(config-if)# speed 100

This example shows how to allow Fast Ethernet interface 5/4 to autonegotiate the speed and duplex mode:

```
Switch(config)# interface fastethernet 5/4
Switch(config-if)# speed auto
```

```
<u>Note</u>
```

The speed auto 10 100 command is similar to the speed auto command on a Fast Ethernet interface.

This example shows how to limit the interface speed to 10 and 100 Mbps on the Gigabit Ethernet interface 1/1 in auto-negotiation mode:

```
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# speed auto 10 100
```

This example shows how to limit the speed negotiation to 100 Mbps on the Gigabit Ethernet interface 1/1:

```
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# speed auto 100
```

Commands Command Description duplex Configures the duplex operation on an interface. interface (refer to Cisco IOS documentation) Configures an interface type and enter interface configuration mode. show controllers (refer to Cisco IOS documentation) Displays controller information. show interfaces Displays traffice on a specific interface.

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. To disable storm control for the broadcast traffic and to disable a specified storm-control action, use the **no** form of this command.

storm-control {broadcast level high level [lower level]} | action {shutdown | trap}}

no storm-control {broadcast level [lower level]} | action {shutdown | trap}}

Syntax Description	broadcast	Enables the broadcast storm control on the port.
	level high-level lo	<i>ver-level</i> Defines the rising and falling suppression levels:
		• <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.
Command Modes	Interface configura	tion mode Modification
-	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch
	12.2(40)SG	Support for the Supervisor Engine 6-E and Catalyst 4900M chassis is introduced.
Usage Guidelines		ntrol broadcast level command to enable traffic storm control on the interface, c storm control level, and apply the traffic storm control level to the broadcast traffic

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.

The lower level is ignored for the interfaces that perform storm control in the hardware.

Note

The **lower level** keyword does not apply to the Supervisor Engine 6-E and Catalyst 4900M chassis implementations.

Examples

This example shows how to enable broadcast storm control on a port with a 75.67 percent rising suppression level:

```
Switch# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 3/1
Switch(config-if)# storm-control broadcast level 75.67
Switch(config-if)# end
```

This example shows how to disable the port during a storm:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 3/1
Switch(config-if)# storm-control action shutdown
Switch(config-if)# end
```

This example shows how to disable storm control on a port:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 3/1
Switch(config-if)# no storm-control broadcast level
Switch(config-if)# end
```

This example shows how to disable storm control by setting the high level to 100 percent:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 3/1
Switch(config-if)# storm-control broadcast level 100
Switch(config-if)# end
```

Related Commands	Command	Description	
show interfaces counters		Displays the traffic on the physical interface.	
	show running-config	Displays the running configuration of a switch.	

L

storm-control broadcast include multicast

To enable multicast storm control on a port, use the **storm-control broadcast include multicast** command. To disable multicast storm control, use the **no** form of this command.

storm-control broadcast include multicast

no storm-control broadcast include multicast

Defaults Multicast storm control is disabled.

Command ModesGlobal configuration modeInterface configuration mode on a Supervisor Engine 6-E or Catalyst 4900M chassis

 Release
 Modification

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

 12.2(40)SG
 Support for the Supervisor Engine 6-E and Catalyst 4900M chassis is introduced.

Usage Guidelines This command prompts the hardware to filter multicast packets if it is already filtering broadcast packets.

The Supervisor Engine 6-E and Catalyst 4900M chassis supports per-interface multicast suppression. When you enable multicast suppression on an interface you subject incoming multicast and broadcast traffic on that interface to suppression.

Examples

This example shows how to enable multicast storm control globally:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# storm-control broadcast include multicast
Switch(config)# end
```

This example shows how to enable per-port Multicast storm control on a Supervisor Engine 6-E:

Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# interface fastethernet2/4 Switch(config-if)# storm-control broadcast include multicast Switch(config)# end

Related Commands

Command	Description
storm-control	Enables broadcast storm control on a port and and specifies
	what to do when a storm occurs on a port.

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 vlan_num	(Optional) Sets the VLAN when the interface is in access mode; valid values are from 1 to 1005.	
	nonegotiate	(Optional) Specifies that the DISL/DTP negotiation packets will not be sent on the interface.	
	voice vlan <i>vlan_id</i>	(Optional) Specifies the number of the VLAN; valid values are from 1 to 1005.	
	dot1p	(Optional) Specifies that the PVID packets are tagged as priority.	
	none	(Optional) Specifies that the telephone and voice VLAN do not communicate.	
	untagged	(Optional) Specifies the untagged PVID packets.	
		on parameter is set to auto. I trunk interface native VLANs are a default VLAN corresponding to the platform are.	
	• All VLAN lists include all VLANs.		
	• No voice VLAN is	enabled.	
Command Modes	Interface configuration	mode	
Command History	Release Mod	ification	
	12.1(8a)EW Supp	port for this command was introduced on the Catalyst 4500 series switch.	

Support for voice VLAN was added.

12.1(11)EW

Usage Guidelines	The no switchport command shuts the port down and then reenables 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 the 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 stop 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, which is 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, which is configured as a switched interface, to refrain from negotiating in 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
---------	----------

Command	Description	
show interfaces switchport	Displays the administrative and operational status of a	
	switching (nonrouting) port.	

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	vlan-id	(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 set	tings are as follows:	
		VLAN and trunk interface native VLAN are default VLANs that correspond to the r the interface hardware.	
	• All VLAN	lists include all VLANs.	
Command Modes	Interface confi	guration mode	
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.	
		the switchport command without any keywords to configure the LAN interface as a ce before you can enter the switchport access vlan command. This action is required only 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 appropria default VLAN for the device. If your system is configured with a Supervisor Engine I, valid values for <i>vlan-id</i> are from 1 to 1005. your system is configured with a Supervisor Engine II, valid values for <i>vlan-id</i> are from 1 to 4094. Extended-range VLANs are not supported on systems configured with a Supervisor Engine I.		

Examples	This example shows how to cause the port interface to stop operating as a Cisco-routed port and convert to a Layer 2-switched interface: Switch(config-if)# switchport Switch(config-if)# 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.		
Note			
	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 a Switch(config-if)#	ccess vlan 2	
Related Commands	Command	Description	
	show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.	

I

switchport autostate exclude

To exclude a port from the VLAN interface link-up calculation, use the **switchport autostate exclude** command. To return to the default settings, use the **no** form of this command.

switchport autostate exclude

no switchport autostate exclude

	no switchpo	ort autostate exclude		
Syntax Description	This command has no keywords or arguments.			
Defaults	All ports are included in the VLAN interface link-up calculation.			
Command Modes	Interface configuration mode			
Command History	Release	Modification		
	12.2(37)SG	Support for this command was introduced on the Catalyst 4500 series switch		
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 autostate exclude command. This action is required only if you have not entered the switchport command for the interface.			
Note	The switchport 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.			
	The switchport autostate exclude command marks the port to be excluded from the interface VLAN up calculation when there are multiple ports in the VLAN.			
		face <i>interface</i> switchport command displays the autostate mode if the mode has been has not been set, the autostate mode is not displayed.		
Examples	This example sh	nows how to exclude a port from the VLAN interface link-up calculation:		
	Switch(config-if)# switchport autostate exclude Switch(config-if)#			
	This example shows how to include a port in the VLAN interface link-up calculation:			
	Switch(config-if)# no switchport autostate exclude Switch(config-if)#			
	You can verify y	your settings by entering the show interfaces switchport privileged EXEC command.		

Related Commands	Command	Description	
	show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.	
		s (nom o dang) porti	

switchport block

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

switchport block {multicast | unicast}

no switchport block {multicast | unicast}

Syntax Description	multicast	Specifies that the unknown multicast traffic should be blocked.		
	unicast	Specifies that the unknown unicast traffic should be blocked.		
Defaults	Unknown multicast	t and unicast traffic are not blocked.		
	All traffic with unk	known MAC addresses is sent to all ports.		
Command Modes	Interface 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 block the unknown multicast or unicast traffic on the switch ports. Blocking the unknown multicast or unicast traffic is not automatically enabled on the switch ports; you must explicitly configure it.			
Note		tion about blocking the packets, refer to the software configuration guide for this		
Examples	This example shows how to block the unknown multicast traffic on an interface: Switch(config-if)# switchport block multicast You can verify your setting by entering the show interfaces interface-id switchport privileged EXEC command.			
Related Commands	Command	Description		
	show interfaces sy	witchport Displays the administrative and operational status of a switching (nonrouting) port.		

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 this command.

switchport mode {access | dot1q-tunnel | trunk | dynamic {auto | desirable}}

switchport mode private-vlan {host | promiscuous | trunk promiscuous | trunk [secondary]}

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 become 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 promiscuous	Specifies that the ports with valid PVLAN trunk mapping become active promiscuous trunk ports.
	private-vlan trunk secondary	Specifies that the ports with a valid PVLAN trunk association become active host private VLAN trunk ports.

Defaults Link converts to a trunk link.

dot1q tunnel ports are disabled.

Command Modes Interface configuration mode

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.
	12.2(31)SG	Support was added for trunk promiscuous 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 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:The port does not have a valid PVLAN association.The port does not have valid allowed normal VLANs.				
	Examples	This example shows how to set the interface to dynamic desirable mode:									
	Examples	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 dotlq-tunnel Switch(config-if)#										
	This example shows how to configure a promiscuous trunk port:										
	Switch(config-if)# switchport mode private-vlan trunk promiscuous Switch(config-if)#										
	This example shows how to configure an isolated trunk port:										
	Switch(config-if)# switchport mode private-vlan trunk										
	OR Switch(config-if)# switchport mode private-vlan trunk secondary 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.										
This example shows how to configure interface FastEthernet 5/2 as a PVLAN promiscuous port, map it to a PVLAN, and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if) # switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 200 2
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name:Fa5/2
Switchport:Enabled
Administrative Mode:private-vlan promiscuous
Operational Mode:private-vlan promiscuous
Administrative Trunking Encapsulation:negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking:Off
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Voice VLAN:none
Administrative Private VLAN Host Association:none
Administrative Private VLAN Promiscuous Mapping:200 (VLAN0200) 2 (VLAN0002)
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
Operational Private VLANs:
  200 (VLAN0200) 2 (VLAN0002)
Trunking VLANs Enabled:ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed:ALL
```

This example shows how to configure interface FastEthernet 5/1 as a PVLAN host port and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 202 440
Switch(config-if)# end
```

```
Switch# show interfaces fastethernet 5/1 switchport
Name: Fa5/1
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Appliance trust: none
Administrative Private Vlan
  Host Association: 202 (VLAN0202) 440 (VLAN0440)
  Promiscuous Mapping: none
  Trunk encapsulation : dot1q
  Trunk vlans:
Operational private-vlan(s):
  202 (VLAN0202) 440 (VLAN0440)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

L

This example shows how to configure interface FastEthernet 5/2 as a secondary trunk port, and verify the configuration:

```
Switch# configure terminal
Switch(config) # interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan trunk secondary
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if) # switchport private-vlan trunk allowed vlan 10. 3-4
Switch(config-if)# switchport private-vlan association trunk 3 301
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
   Switchport: Enabled
   Administrative Mode: private-vlan trunk secondary
   Operational Mode: private-vlan trunk secondary
   Administrative Trunking Encapsulation: negotiate
   Operational Trunking Encapsulation: dotlq
   Negotiation of Trunking: On
   Access Mode VLAN: 1 (default)
   Trunking Native Mode VLAN: 1 (default)
   Administrative Native VLAN tagging: enabled
   Voice VLAN: none
   Administrative private-vlan host-association: none A
   dministrative private-vlan mapping: none
   Administrative private-vlan trunk native VLAN: 10
   Administrative private-vlan trunk Native VLAN tagging: enabled
   Administrative private-vlan trunk encapsulation: dotlq
   Administrative private-vlan trunk normal VLANs: none
   Administrative private-vlan trunk associations:
       3 (VLAN0003) 301 (VLAN0301)
   Administrative private-vlan trunk mappings: none
   Operational private-vlan: none
   Operational Normal VLANs: none
   Trunking VLANs Enabled: ALL
   Pruning VLANs Enabled: 2-1001
   Capture Mode Disabled Capture VLANs Allowed: ALL
   Unknown unicast blocked: disabled
   Unknown multicast blocked: disabled
   Appliance trust: none
```

Switch(config-if)#

This example shows how to configure interface FastEthernet 5/2 as a promiscuous trunk port and to verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan trunk promiscuous
Switch(config-if) # switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 10, 3-4
Switch(config-if)# switchport private-vlan mapping trunk 3 301, 302
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
Switchport: Enabled
Administrative Mode: private-vlan trunk promiscuous
Operational Mode: private-vlan trunk promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dotlq
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

```
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: 10
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dotlq
Administrative private-vlan trunk normal VLANs: 3-4,10
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings:
    3 (VLAN0003) 301 (VLAN0301) 302 (VLAN0302)
Operational private-vlan:
  3 (VLAN0003) 301 (VLAN0301) 302 (VLAN0302)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Unknown unicast blocked: disabled
```

Unknown unicast blocked: disabled Unknown multicast blocked: disabled Appliance trust: none Switch(config-if)#

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport	Enables port security on an interface.
switchport private-vlan	Defines a PVLAN association for an isolated or community
host-association	port.
switchport private-vlan mapping	Defines private VLAN mapping for a promiscuous port.

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 [vlan {access | voice} |
 mac-address sticky [mac-address] [vlan access | voice] | maximum value [vlan {access |
 voice} | 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 [vlan {access | voice} | mac-address sticky [mac-address] [vlan access | voice] | maximum value [vlan {access | voice} | 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 time	(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 mac-address	(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 the dynamic addresses as sticky on the interface.
	vlan access	(Optional) Deletes the secure MAC addresses from access VLANs.
	vlan voice	(Optional) Deletes the secure MAC addresses from voice VLANs.
	maximum value	(Optional) Sets the maximum number of secure MAC addresses for the interface. Valid values are from 1 to 3072. 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.

	The default settings are as follows:		
	• Port security is	disabled.	
	• When port secu MAC addresses	rity is enabled and no keywords are entered, the default maximum number of secures s is 1.	
	• Aging is disabl	ed.	
	 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 configurat	tion mode	
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.	
	12.2(31)SG	Add support for sticky port security.	
Usage Guidelines	After you set the maximum number of secure MAC addresses that are 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.		
	The packets are dro	pped into the hardware when the maximum number of secure MAC addresses are in d a station that does not have a MAC address in the address table attempts to access	
	The packets are dro the address table an the interface. If you enable port so	pped into the hardware when the maximum number of secure MAC addresses are in	
	The packets are dro the address table an the interface. If you enable port so the maximum allow	pped into the hardware when the maximum number of secure MAC addresses are in d a station that does not have a MAC address in the address table attempts to access ecurity on a voice VLAN port and if there is a PC connected to the IP phone, you se	
	The packets are dro the address table an the interface. If you enable port so the maximum allow You cannot configu	pped into the hardware when the maximum number of secure MAC addresses are in id a station that does not have a MAC address in the address table attempts to access ecurity on a voice VLAN port and if there is a PC connected to the IP phone, you se yed secure addresses on the port to more than 1.	
	The packets are dro the address table an the interface. If you enable port so the maximum allow You cannot configu A secure port has th	pped into the hardware when the maximum number of secure MAC addresses are in id a station that does not have a MAC address in the address table attempts to access ecurity on a voice VLAN port and if there is a PC connected to the IP phone, you se red secure addresses on the port to more than 1. re static secure MAC addresses in the voice VLAN.	
	 The packets are drop the address table and the interface. If you enable port so the maximum allow You cannot configu A secure port has the A secure port continue to the table port continue to table port port port port port port port port	pped into the hardware when the maximum number of secure MAC addresses are in d a station that does not have a MAC address in the address table attempts to access ecurity on a voice VLAN port and if there is a PC connected to the IP phone, you se red secure addresses on the port to more than 1. re static secure MAC addresses in the voice VLAN. he following limitations:	
	 The packets are drop the address table and the interface. If you enable port so the maximum allow You cannot configure A secure port has the A secure port configure A secure A secu	pped into the hardware when the maximum number of secure MAC addresses are in d a station that does not have a MAC address in the address table attempts to access ecurity on a voice VLAN port and if there is a PC connected to the IP phone, you se yed secure addresses on the port to more than 1. re static secure MAC addresses in the voice VLAN. he following limitations: annot be a dynamic access port or a trunk port.	
	 The packets are drop the address table and the interface. If you enable port so the maximum allow You cannot configure A secure port has the A secure port configure A secure A secure port configure A secure A s	pped into the hardware when the maximum number of secure MAC addresses are in d a station that does not have a MAC address in the address table attempts to access ecurity on a voice VLAN port and if there is a PC connected to the IP phone, you se yed secure addresses on the port to more than 1. re static secure MAC addresses in the voice VLAN. the following limitations: eannot be a dynamic access port or a trunk port. eannot be a routed port.	
	 The packets are drop the address table and the interface. If you enable port so the maximum allow You cannot configu A secure port has the A secure port c 	pped into the hardware when the maximum number of secure MAC addresses are in d a station that does not have a MAC address in the address table attempts to access ecurity on a voice VLAN port and if there is a PC connected to the IP phone, you se yed secure addresses on the port to more than 1. re static secure MAC addresses in the voice VLAN. the following limitations: exannot be a dynamic access port or a trunk port. exannot be a protected port.	
	 The packets are drop the address table and the interface. If you enable port so the maximum allow You cannot configure A secure port has the A secure port control of A secure port a secure port a secure port control of A secure port a secure port a secure port a secure port a s	pped into the hardware when the maximum number of secure MAC addresses are in d a station that does not have a MAC address in the address table attempts to access ecurity on a voice VLAN port and if there is a PC connected to the IP phone, you se yed secure addresses on the port to more than 1. re static secure MAC addresses in the voice VLAN. ne following limitations: annot be a dynamic access port or a trunk port. cannot be a routed port. cannot be a protected port. cannot be a destination port for Switched Port Analyzer (SPAN).	

• 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 reenable 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 action 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 that are 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 set the aging time to 2 hours (120 minutes) for the secure addresses on the Fast Ethernet port 12:

```
Switch(config)# interface fastethernet 0/12
Switch(config-if)# switchport port-security aging time 120
Switch(config-if)#
```

This example shows how to set the aging timer type to Inactivity for the secure addresses on the Fast Ethernet port 12:

```
Switch(config)# interface fastethernet 0/12
Switch(config-if)# switch port-security aging type inactivity
Switch(config-if)#
```

The following example shows how to configure rate limit for invalid source packets on Fast Ethernet port 12:

```
Switch(config)# interface fastethernet 0/12
Switch(config-if)# switchport port-security limit rate invalid-source-mac 100
Switch(config-if)#
```

The following example shows how to configure rate limit for invalid source packets on Fast Ethernet port 12:

```
Switch(config)# interface fastethernet 0/12
Switch(config-if)# switchport port-security limit rate invalid-source-mac none
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 remove all sticky and static addresses that are 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)
```

This example shows how to make all MAC addresses learned on Fast Ethernet port 12 sticky:

```
Switch(config)# interface fastethernet 2/12
SSwitch(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)
```

```
<u>Note</u>
```

This command makes all sticky addresses on this interface normal learned entries. It does not delete the entries from the secure MAC address table.

Note

The following examples show how to configure sticky secure MAC addresses in access and voice VLANs on interfaces with voice VLAN configured. If you do not have voice VLAN configured the **vlan** [access | voice] keywords are not supported.

This example shows how to configure sticky MAC addresses for voice and data VLANs on Fast Ethernet interface 5/1 and to verify the configuration:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fa5/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.obob vlan voice
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.obob vlan access
Switch(config-if)# end
```

This example shows how to designate a maximum of one MAC address for a voice VLAN (for a Cisco IP Phone, let's say) and one MAC address for the data VLAN (for a PC, let's say) on Fast Ethernet interface 5/1 and to verify the configuration:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fa5/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security maximum 1 vlan voice
Switch(config-if)# switchport port-security maximum 1 vlan access
Switch(config-if)# end
```



Sending traffic to the ports causes the system to configure the port with sticky secure addresses.

You can verify your settings by using the show port-security address privileged EXEC command.

Related Commands	Command	Description
	show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
	show port-security	Displays the port security settings for an interface or for the switch.
	switchport block	Prevents the unknown multicast or unicast packets from being forwarded.

switchport private-vlan association trunk

To configure the association between a secondary VLAN 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 this 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 private VLAN relationship.
oymax booonprion	secondary-vlan-id	Number of the secondary VLAN of the private VLAN relationship.
Defaults	Private VLAN mapping is disabled.	
Command Modes	Interface configuration mode	
Command History	Release	Nodification
	12.1(12c)EW S	Support for this command was introduced on the Catalyst 4500 series switch
	12.2(20)EW S	Support for community VLAN was added.
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. Only isolated secondary VLANs can be carried over a private VLAN trunk.	
<u>Note</u>	Community second	ary VLANs on a private VLAN trunk are not supported in this release.
	If there is no trunk	association, any packets received on the secondary VLANs are dropped.
	This example shows how to configure a port with a primary VLAN (VLAN 18) and secondary V (VLAN 20).	
Examples	This example shows (VLAN 20):	s how to configure a port with a primary VLAN (VLAN 18) and secondary VLAN
Examples	(VLAN 20):	# switchport private-vlan association trunk 18 20
Examples	(VLAN 20): Switch(config-if) Switch(config-if)	# switchport private-vlan association trunk 18 20

This example shows how to configure interface FastEthernet 5/2 as a secondary trunk port, and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan trunk secondary
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 10. 3-4
Switch(config-if)# switchport private-vlan association trunk 3 301
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
   Switchport: Enabled
   Administrative Mode: private-vlan trunk secondary
   Operational Mode: private-vlan trunk secondary
   Administrative Trunking Encapsulation: negotiate
   Operational Trunking Encapsulation: dot1q
   Negotiation of Trunking: On
   Access Mode VLAN: 1 (default)
   Trunking Native Mode VLAN: 1 (default)
   Administrative Native VLAN tagging: enabled
   Voice VLAN: none
   Administrative private-vlan host-association: none A
   dministrative private-vlan mapping: none
   Administrative private-vlan trunk native VLAN: 10
   Administrative private-vlan trunk Native VLAN tagging: enabled
   Administrative private-vlan trunk encapsulation: dotlq
   Administrative private-vlan trunk normal VLANs: none
   Administrative private-vlan trunk associations:
       3 (VLAN0003) 301 (VLAN0301)
   Administrative private-vlan trunk mappings: none
   Operational private-vlan: none
   Operational Normal VLANs: none
   Trunking VLANs Enabled: ALL
   Pruning VLANs Enabled: 2-1001
   Capture Mode Disabled Capture VLANs Allowed: ALL
   Unknown unicast blocked: disabled
```

Unknown multicast blocked: disabled Appliance trust: none Switch(config-if)#

Related Commands	Command	Description
	show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
	switchport mode	Enables the interface type.

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 this command.

switchport private-vlan host-association {primary-vlan-id} {secondary-vlan-id}

no switchport private-vlan host-association

Syntax Description	primary-vlan-id	Number of the primary VLAN of the PVLAN relationship; valid values are from 1 to 4094.
	secondary-vlan-list	Number of the secondary VLAN of the private VLAN relationship; valid values are from 1 to 4094.
Defaults	Private VLAN map	ping is disabled.
Command Modes	Interface configuration mode	
Command History	Release	Nodification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW S	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 is do not exist, the command is allowed, but the port is made inactive.
Usage Guidelines	There is no runtime mode but all VLAN	•
Usage Guidelines Examples	There is no runtime mode but all VLAN The secondary VLA	
	There is no runtime mode but all VLAN The secondary VLA This example shows (VLAN 20):	is do not exist, the command is allowed, but the port is made inactive. AN may be an isolated or community VLAN. s how to configure a port with a primary VLAN (VLAN 18) and secondary VLAN # switchport private-vlan host-association 18 20
	There is no runtime mode but all VLAN The secondary VLA This example shows (VLAN 20): Switch(config-if) Switch(config-if)	is do not exist, the command is allowed, but the port is made inactive. AN may be an isolated or community VLAN. s how to configure a port with a primary VLAN (VLAN 18) and secondary VLAN # switchport private-vlan host-association 18 20

This example shows how to configure interface FastEthernet 5/1 as a PVLAN host port and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 202 440
Switch(config-if)# end
Switch# show interfaces fastethernet 5/1 switchport
Name: Fa5/1
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Appliance trust: none
Administrative Private Vlan
 Host Association: 202 (VLAN0202) 440 (VLAN0440)
  Promiscuous Mapping: none
 Trunk encapsulation : dot1q
 Trunk vlans:
Operational private-vlan(s):
  202 (VLAN0202) 440 (VLAN0440)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

Related Commands	Command	Description
	show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
	switchport mode	Enables the interface type.

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}

switchport private-vlan mapping trunk {primary-vlan-id} [add | remove] secondary-vlan-list

no switchport private-vlan mapping [trunk]

Syntax Description	primary-vlan-id	Number of the primary VLAN of the private VLAN relationship; valid values are from 2 to 4094 (excluding 1002 to 1005).
	secondary-vlan-list	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 the secondary VLANs and the primary VLAN.
	trunk	Maps the trunks secondary VLANs to the primary VLAN.
Defaults Command Modes	Private VLAN mapp	
	Interface configurati	
Command Modes	Interface configurati	on mode
Command Modes	Interface configurati	on mode Iodification
Command Modes	Interface configuration Release N 12.1(8a)EW S 12.1(12c)EW S	on mode Iodification upport for this command was introduced on the Catalyst 4500 series switch

Usage Guidelines

There is no run-time effect on the port unless it is in private VLAN promiscuous mode. If the port is in private VLAN 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.

The maximum number of unique private VLAN pairs supported by the **switchport private-vlan mapping trunk** command above is 500. For example, one thousand secondary VLANs could map to one primary VLAN, or one thousand secondary VLANs could map one to one to one thousand primary VLANs.

<u>Note</u>

Examples This example shows how to configure the mapping of primary VLAN 18 to the secondary isolated VLAN 20 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)#

This example shows how to add a range of secondary VLANs to the mapping:

```
Switch(config-if)# switchport private-vlan mapping 18 add 22-24
Switch(config-if)#
```

This example shows how to add a range of secondary VLANs to the trunk mapping:

```
Switch(config-if)# switchport private-vlan mapping trunk 18 add 22-24
Switch(config-if)#
```

This example shows how to configure interface FastEthernet 5/2 as a PVLAN promiscuous port, map it to a PVLAN, and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 200 2
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name:Fa5/2
Switchport:Enabled
Administrative Mode:private-vlan promiscuous
Operational Mode:private-vlan promiscuous
Administrative Trunking Encapsulation:negotiate
Operational Trunking Encapsulation:native
Negotiation of Trunking:Off
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Voice VLAN:none
Administrative Private VLAN Host Association:none
Administrative Private VLAN Promiscuous Mapping:200 (VLAN0200) 2 (VLAN0002)
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
Operational Private VLANs:
 200 (VLAN0200) 2 (VLAN0002)
Trunking VLANs Enabled:ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed:ALL
```

This example shows how to configure interface FastEthernet 5/2 as a promiscuous trunk port and to verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if) # switchport mode private-vlan trunk promiscuous
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 10, 3-4
Switch(config-if)# switchport private-vlan mapping trunk 3 301, 302
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
Switchport: Enabled
Administrative Mode: private-vlan trunk promiscuous
Operational Mode: private-vlan trunk promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: 10
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: 3-4,10
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings:
   3 (VLAN0003) 301 (VLAN0301) 302 (VLAN0302)
Operational private-vlan:
  3 (VLAN0003) 301 (VLAN0301) 302 (VLAN0302)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

Unknown unicast blocked: disabled Unknown multicast blocked: disabled Appliance trust: none Switch(config-if)#

Related Commands	Command	Description
	show interfaces private-vlan mapping	Displays PVLAN mapping information for VLAN SVIs.

switchport private-vlan trunk allowed vlan

To configure a list of the allowed normal VLANs on a private VLAN trunk port, use the **switchport private-vlan trunk allowed vlan** command. To remove all the allowed normal VLANs from a private VLAN trunk port, use the **no** form of this 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		
	vlan_list	Sets the list of allowed VLANs; see the "Usage Guidelines" section 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.
	vlan_atom	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 configu	
	Interface configu	
		uration mode
Command History	Release 12.1(12c)EW	uration mode Modification Support for this command was introduced on the Catalyst 4500 series switch
Command History	Release 12.1(12c)EW By default, no no	uration mode Modification Support for this command was introduced on the Catalyst 4500 series switch ormal VLANs are allowed unless you explicitly configure the VLANs to be allowed.
Command Modes Command History Usage Guidelines	Release 12.1(12c)EW By default, no no Use this comman	uration mode Modification Support for this command was introduced on the Catalyst 4500 series switch

Examples

This example shows how to configure the 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 the allowed normal VLANs from a private VLAN trunk port:

```
Switch(config-if)# no switchport private-vlan trunk allowed vlan
Switch(config-if)#
```

This example shows how to configure interface FastEthernet 5/2 as a secondary trunk port, and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if) # switchport mode private-vlan trunk secondary
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 10. 3-4
Switch(config-if)# switchport private-vlan association trunk 3 301
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
   Switchport: Enabled
   Administrative Mode: private-vlan trunk secondary
   Operational Mode: private-vlan trunk secondary
   Administrative Trunking Encapsulation: negotiate
   Operational Trunking Encapsulation: dotlq
   Negotiation of Trunking: On
   Access Mode VLAN: 1 (default)
   Trunking Native Mode VLAN: 1 (default)
   Administrative Native VLAN tagging: enabled
   Voice VLAN: none
   Administrative private-vlan host-association: none A
   dministrative private-vlan mapping: none
   Administrative private-vlan trunk native VLAN: 10
   Administrative private-vlan trunk Native VLAN tagging: enabled
   Administrative private-vlan trunk encapsulation: dotlq
   Administrative private-vlan trunk normal VLANs: none
   Administrative private-vlan trunk associations:
       3 (VLAN0003) 301 (VLAN0301)
   Administrative private-vlan trunk mappings: none
   Operational private-vlan: none
   Operational Normal VLANs: none
   Trunking VLANs Enabled: ALL
   Pruning VLANs Enabled: 2-1001
   Capture Mode Disabled Capture VLANs Allowed: ALL
   Unknown unicast blocked: disabled
   Unknown multicast blocked: disabled
   Appliance trust: none
Switch(config-if)#
```

L

This example shows how to configure interface FastEthernet 5/2 as a promiscuous trunk port and to verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if) # switchport mode private-vlan trunk promiscuous
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 10, 3-4
Switch(config-if)# switchport private-vlan mapping trunk 3 301, 302
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
Switchport: Enabled
Administrative Mode: private-vlan trunk promiscuous
Operational Mode: private-vlan trunk promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: 10
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: 3-4,10
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings:
   3 (VLAN0003) 301 (VLAN0301) 302 (VLAN0302)
Operational private-vlan:
  3 (VLAN0003) 301 (VLAN0301) 302 (VLAN0302)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

Unknown unicast blocked: disabled Unknown multicast blocked: disabled Appliance trust: none Switch(config-if)#

Related Commands	Command	Description
	show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
	switchport mode	Enables the interface type.

switchport private-vlan trunk native vlan tag

To control the tagging of the 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 this command.

switchport private-vlan trunk native vlan tag

no switchport private-vlan trunk native vlan tag

Defaults The default setting is global; the settings on the port are determined by the global setting.

Command Modes Interface configuration mode

Command History	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	Command	Description
	show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
	switchport mode	Enables the interface type.

switchport trunk

To set the 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 the "Usage Guidelines" section 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 the "Usage Guidelines" section for formatting guidelines for <i>vlan_list</i> .

Defaults

The default settings are as follows:

- The encapsulation type is dependent on the platform or interface hardware.
- The access VLANs and trunk interface native VLANs are a default VLAN that corresponds to the platform or the interface hardware.
- All VLAN lists include all VLANs.
- Native VLAN tagging is enabled on the port if enabled globally.

Command Modes Interface configuration mode

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 <i>vlan_list</i> fo	rmat is all none [add remove except] <i>vlan_atom[,vlan_atom</i>], where:
	1	s all VLANs from 1 to 4094. This keyword is not supported on commands that do not /LANs in the list to be set at the same time.
		tes an empty list. This keyword is not supported on commands that require certain be set or at least one VLAN to be set.
	• add adds th	e defined list of VLANs to those currently set, instead of replacing the list.
	• remove rem	noves 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.
		is either a single VLAN number from 1 to 4094 or a continuous range of VLANs y two VLAN numbers (the lesser one first, separated by a hyphen).
	-	trunk encapsulation command is supported only for platforms and interface hardware both ISL and 802.1Q formats.
	•	negotiate keywords, and DISL and DTP negotiation do not resolve the encapsulation ne selected format. The no form of this command resets the trunk encapsulation format ult.
	The no form of t for the device.	he native vlan command resets the native mode VLAN to the appropriate default VLAN
	The no form of	the allowed vlan command resets the list to the default list, which allows all VLANs.
	The no form of for VTP pruning	the pruning vlan command resets the list to the default list, which enables all VLANs g.
		tion guidelines and restrictions apply when using 802.1Q trunks and impose some ne trunking strategy for a network:
	802.1Q trun	ecting Cisco switches through an 802.1Q trunk, make sure that the native VLAN for an ik is the same on both ends of the trunk link. If the native VLAN on one end of the trunk from the native VLAN on the other end, spanning-tree loops might result.
	every VLA tree enablec on every VI	panning tree on the native VLAN of an 802.1Q trunk without disabling spanning tree on N in the network can cause spanning-tree loops. We recommend that you leave spanning d on the native VLAN of an 802.1Q trunk. If this is not possible, disable spanning tree LAN in the network. Make sure that your network is free of physical loops before banning tree.
	BPDUs on a are sent unt (01-80-C2-0	connect two Cisco switches through 802.1Q trunks, the switches exchange spanning-tree each VLAN that is allowed on the trunks. The BPDUs on the native VLAN of the trunk agged to the reserved 802.1d spanning-tree multicast MAC address 00-00-00). The BPDUs on all other VLANs on the trunk are sent tagged to the reserved cast 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 the 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 that are connected to the non-Cisco 802.1Q network through the 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 the 802.1Q trunks. You cannot connect Cisco switches to a non-Cisco 802.1Q network through the ISL trunks or through the 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.

Follow these guidelines for native VLAN tagging:

- 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 reenable 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 that 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 that is 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)#
```

This example shows how to configure a secure MAC-address and a maximum limit of secure MAC addresses on Gigabit Ethernet port 1 for all VLANs:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 3
```

This example shows how to configure a secure MAC-address on Gigabit Ethernet port 1 in a specific VLAN or range of VLANs:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# vlan-range 2-6
Switch(config-if-vlan-range)# port-security maximum 3
```

This example shows how to configure a secure MAC-address in a VLAN on Gigabit Ethernet port 1:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# vlan-range 2-6
Switch(config-if-vlan-range)# port-security mac-address 1.1.1
Switch(config-if-vlan-range)# port-security mac-address sticky 1.1.2
Switch(config-if-vlan-range)# port-security mac-address sticky 1.1.3
```

You can verify your settings by using the **show port-security interface vlan** privileged EXEC command.

Related Commands	Command	Description
	show interfaces switchport	Displays the administrative and operational status of a
		switching (nonrouting) port.

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	datagram-size	Layer 2 payload size; valid values from 1500 to 1552 bytes.		
Defaults	The default MT	J setting is 1500 bytes.		
Command Modes	Global configuration mode			
Command History	Release	Modification		
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.		
the Layer 3 MTU is changed as a result of changing the sy		<i>ize</i> parameter specifies the Ethernet payload size, not the total Ethernet frame size, and J is changed as a result of changing the system mtu command.		
	For ports from 3 to18 on 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.			
	For other modules, an Ethernet payload size of up to 1552 bytes is supported with a total Ethernet fra size of up to 1600 bytes.			
Examples	This example sh	ows how to set the MTU size to 1550 bytes:		
	Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# system mtu 1550 Switch(config)# end Switch#			
	This example shows how to revert to the default MTU setting:			
		ation commands, one per line. End with CNTL/Z. # no system mtu		

Related Commands	Command	Description	
	show interfaces	Displays traffic on a specific interface.	
	show system mtu	Displays the global MTU setting.	

test cable-diagnostics tdr

To test the condition of copper cables on 48-port 10/100/1000 BASE-T modules, use the **test cable-diagnostics tdr** command.

test cable-diagnostics tdr {interface {interface interface-number}

Note	This command will be deprecated in future Cisco IOS releases. Please use the diagnostic start command.		
Syntax Description	interface <i>interface</i> Interface type; valid values are fastethernet and gigabitethernet .		
	<i>interface-number</i> Module and port number.		
Defaults	This command has no default settings.		
Command Modes	Privileged EXEC mode		
Command History	Release Modification		
	12.2(25)SGSupport for this command on the Catalyst 4500 series switch.		
Usage Guidelines	The TDR test is supported on Catalyst 4500 series switches running Cisco IOS Release 12.2(25)SG for the following line cards only:		
	• WS-X4548-GB-RJ45		
	• WS-X4548-GB-RJ45V		
	• WS-X4524-GB-RJ45V		
	• WS-X4013+TS		
	• WS-C4948		
	• WS-C4948-10GE		
	The valid values for interface <i>interface</i> are fastethernet and gigabitethernet .		
	Do not start the test at the same time on both ends of the cable. Starting the test at both ends of the cable at the same time can lead to false test results.		
	Do not change the port configuration during any cable diagnostics test. This action may result in incorrect test results.		
	The interface must be operating before starting the TDR test. If the port is down, the results of the test will be invalid. Issue the no shutdown command on the port.		

Examples	This example shows how to start th	e TDR test on port 1 on module 2:		
	Switch# test cable-diagnostics Switch#	Switch# test cable-diagnostics tdr int gi2/1 Switch# This example shows the message that displays when the TDR test is not supported on a module:		
	This example shows the message the			
•	Switch# test cable-diagnostics 00:03:15:%C4K_IOSDIAGMAN-4-TEST diag tdr test is not supported Switch#	NOTSUPPORTEDONMODULE: Online cable		
<u>Note</u>	will not be available until approxim	The show cable-diagnostic tdr command is used to display the results of a TDR test. The test results will not be available until approximately 1 minute after the test starts. If you enter the show cable-diagnostic tdr command within 1 minute of the test starting, you may see a "TDR test is in progress on interface" message.		
Related Command	s Command	Description		
	show cable-diagnostics tdr	Displays the test results for the TDR cable diagnostics.		

traceroute mac

To display the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address, use the **traceroute mac** command.

traceroute mac [interface *interface-id*] {*source-mac-address*} [**interface** *interface-id*] {*destination-mac-address*} [**vlan** *vlan-id*] [**detail**]

Syntax Description	interface interface-id	(Optional) Specifies the source or destination switch interface.	
	source-mac-address	 MAC address of the source switch in hexadecimal format. MAC address of the destination switch in hexadecimal format. (Optional) Specifies the VLAN on which to trace the Layer 2 path that the packets take from the source switch to the destination switch; valid VLAN IDs are from 1 to 4094. Do not enter leading zeros. 	
	destination-mac-address		
	vlan vlan-id		
	detail	(Optional) Displays detail information.	
Defaults	This command has no defa	ault settings.	
Command Modes	Privileged EXEC mode		
Command History	Release Modifica	ition	
	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 traceroute feature is available on these switches:		
	• Catalyst 2950 switche	s running Release 12.1(12c)EA1 or later	
	• Catalyst 3550 switche	s running Release 12.1(12c)EA1 or later	
	• Catalyst 4500 series switches running Catalyst operating system Release 6.2 or later for the supervisor engine		
	• Catalyst 4500 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 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 traceroute, the switch continues to send Layer 2 trace queries and lets them time out.		
	The maximum number of	hops identified in the path is ten.	
	• •		

Layer 2 traceroute supports only unicast traffic. If you specify a multicast source or destination MAC address, the physical path is not identified, and a 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 a 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 a message appears.

Layer 2 traceroute 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 a 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 Fa0/3 =>Gi0/1con5 (2.2.5.5)) : (2.2.1.1)Gi0/1 =>Gi0/2 con1) : (2.2.1.1)) : (2.2.2.2)) : con2 Gi0/2 => Fa0/1Destination 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# traceroute 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# traceroute 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# traceroute mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
Switch#
```

This example shows the Layer 2 path when the source and destination switches belong to multiple VLANs:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace aborted.
Switch#
```

This example shows how to display the Layer 2 path by specifying the interfaces on the source and destination switches:

```
Switch# traceroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3 0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 (2.2.6.6) : Fa0/1 = Fa0/3
                    (2.2.5.5
                                            Fa0/3 =>Gi0/1
con5
                                    ) :
con1
                    (2.2.1.1
                                    ) :
                                            Gi0/1 =>Gi0/2
                                            Gi0/2 =>Fa0/1
con2
                    (2.2.2.2
                                    ) :
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
Switch#
```

Related Commands	Command	Description
	traceroute mac ip	Displays the Layer 2 path that is taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname.

traceroute mac ip

To display the Layer 2 path that is 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	source-ip-address	IP address of the source switch as a 32-bit quantity in dotted-decimal format.		
	destination-ip-address	IP address of the destination switch as a 32-bit quantity in dotted-decimal format.		
	source-hostname	IP hostname of the source switch.		
	destination-hostname	IP hostname of the destination switch.		
	detail	(Optional) Displays detailed traceroute MAC IP information.		
Defaults	This command has no def	fault settings.		
Command Modes	Privileged EXEC mode			
Command History	Release Modifi	cation		
	12.1(13)EW Suppo	rt for this command was introduced on the Catalyst 4500 series switch.		
Usage Guidelines	The Laver 2 traceroute fe	ature is available on these switches:		
Usage Guidennes	 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 Catalyst 4500 series switches running Catalyst operating system Release 6.2 or later for the supervisor engine 			
	• Catalyst 4500 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 supervisor engine	switches running Catalyst operating system Release 6.1 or later for the		
	supervisor engine	functional properly, Cisco Discovery Protocol (CDP) must be enabled on all		
	supervisor engine For Layer 2 traceroute to the switches in the netwo When the switch detects a	functional properly, Cisco Discovery Protocol (CDP) must be enabled on all		

The **traceroute mac ip** command output shows the Layer 2 path when the specified source and destination IP addresses are in the same subnet. When you specify the IP addresses, the switch uses Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.

- If an ARP entry exists for the specified IP address, the switch uses the associated MAC address and identifies the physical path.
- If an ARP entry does not exist, the switch sends an ARP query and tries to resolve the IP address. The IP addresses must be in the same subnet. If the IP address is not resolved, the path is not identified, and a message appears.

Layer 2 traceroute is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port). When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display the Layer 2 path by specifying the source and destination IP addresses and by using the **detail** keyword:

```
Switch# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac....
2.2.66.66 =>0000.0201.0601
2.2.22.22 =>0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / WS-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# traceroute mac ip con6 con2
Translating IP to mac .....
2.2.66.66 =>0000.0201.0601
2.2.22.22 =>0000.0201.0201
Source 0000.0201.0601 found on con6
con6 (2.2.6.6) :Fa0/1 =>Fa0/3
con5
                    (2.2.5.5)
                                    )
                                      :
                                           Fa0/3 =>Gi0/1
                    (2.2.1.1
con1
                                    )
                                       :
                                           Gi0/1 =>Gi0/2
                    (2.2.2.2
con2
                                    ) :
                                            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# traceroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
Switch#
```

Related Commands	Command	Description
	traceroute mac	Displays the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address.

trust

To define a trust state for traffic classified through the **class** policy-map configuration command, use the **trust** policy-map class configuration command. To return to the default setting, use the **no** form of this command.

trust [cos | dscp]

no trust [cos | dscp]

Syntax Description	COS	Optional) Classify an ingress packet by using the packet class of service (CoS) alue. For an untagged packet, the port default CoS value is used.	
	dscp	(Optional) Classify an ingress packet by using the packet Differentiated Services Code Point (DSCP) values (most significant 6 bits of 8-bit service-type field). For a non-IP packet, the packet CoS value is used if the packet is tagged. If the packet is untagged, the default port CoS value is used to map CoS to DSCP.	
Defaults	The action is not	trusted.	
Command Modes	Policy-map class	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 is	not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.	
	traffic. For exam	d to distinguish the quality of service (QoS) trust behavior for certain traffic from other ple, inbound traffic with certain DSCP values can be trusted. You can configure a class d trust the DSCP values in the inbound traffic.	
	Trust values set v command.	with this command supersede trust values set with the qos trust interface configuration	
		ust cos , QoS uses the received or default port CoS value and the CoS-to-DSCP map to value for the packet.	
	tagged, QoS uses	ist dscp , QoS uses the DSCP value from the ingress packet. For non-IP packets that are the received CoS value; for non-IP packets that are untagged, QoS uses the default port her case, the DSCP value for the packet is derived from the CoS-to-DSCP map.	
	To return to polic use the end com	y-map configuration mode, use the exit command. To return to privileged EXEC mode, mand.	
Examples	This example sho with "class1":	ows how to define a port trust state to trust inbound DSCP values for traffic classified	

```
Switch# configure terminal
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch#
```

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

Related Commands	Command	Description
	class	Specifies the name of the class whose traffic policy you want to create or change.
	police	Configures the Traffic Policing feature.
	policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
	set	Marks IP traffic by setting a class of service (CoS), a Differentiated Services Code Point (DSCP), or IP-precedence in the packet.
	show policy-map	Displays information about the policy map.

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

	• 1		
Syntax Description	queue-id	(Optional) Number of the queue; valid values are from 1 to 4.	
	bandwidth bandwidth-rate	Specifies traffic bandwidth; valid values are from 16000 to 1000000000 bits per second.	
	priority high	Specifies high priority.	
	shape shape-rate	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 follo	ows:	
	• Encapsulation type is dependent on the platform or interface hardware.		
	• QoS enabled bandwidth ra	te is 4:255.	
	• QoS disabled bandwidth rate is 255:1.		
Command Modes	Interface configuration mode		
Command History	Release Modificatio	n	
Command History		n this command was introduced on the Catalyst 4500 series switch	
	12.1(8a)EW Support for	this command was introduced on the Catalyst 4500 series switch	
	12.1(8a)EWSupport forThis command is not supported	this command was introduced on the Catalyst 4500 series switch d on the Supervisor Engine 6-E and Catalyst 4900M chassis.	
Command History Usage Guidelines	12.1(8a)EWSupport forThis command is not supportedThe bandwidth and shape rates	this command was introduced on the Catalyst 4500 series switch d on the Supervisor Engine 6-E and Catalyst 4900M chassis. s cannot exceed the maximum speed of the interface.	
	12.1(8a)EWSupport forThis command is not supportedThe bandwidth and shape ratesThe bandwidth can be configured	this command was introduced on the Catalyst 4500 series switch d on the Supervisor Engine 6-E and Catalyst 4900M chassis. s cannot exceed the maximum speed of the interface. red only on the following:	
	12.1(8a)EWSupport forThis command is not supportedThe bandwidth and shape ratesThe bandwidth can be configure• Uplink ports on Superviso	this command was introduced on the Catalyst 4500 series switch d on the Supervisor Engine 6-E and Catalyst 4900M chassis. c cannot exceed the maximum speed of the interface. red only on the following: r Engine III (WS-X4014)	
	12.1(8a)EWSupport forThis command is not supported The bandwidth and shape rates The bandwidth can be configure • Uplink ports on Superviso • Ports on the WS-X4306-G	this command was introduced on the Catalyst 4500 series switch d on the Supervisor Engine 6-E and Catalyst 4900M chassis. c cannot exceed the maximum speed of the interface. red only on the following: r Engine III (WS-X4014) B module	
	12.1(8a)EWSupport forThis command is not supportedThe bandwidth and shape ratesThe bandwidth can be configure• Uplink ports on Superviso• Ports on the WS-X4306-G• The two 1000BASE-X port	this command was introduced on the Catalyst 4500 series switch d on the Supervisor Engine 6-E and Catalyst 4900M chassis. s cannot exceed the maximum speed of the interface. red only on the following: r Engine III (WS-X4014) B module ts on the WS-X4232-GB-RJ module	
	12.1(8a)EWSupport forThis command is not supportedThe bandwidth and shape ratesThe bandwidth can be configure• Uplink ports on Superviso• Ports on the WS-X4306-G• The two 1000BASE-X port• The first two ports on the V	this command was introduced on the Catalyst 4500 series switch d on the Supervisor Engine 6-E and Catalyst 4900M chassis. a cannot exceed the maximum speed of the interface. red only on the following: r Engine III (WS-X4014) B module ts on the WS-X4232-GB-RJ module WS-X4418-GB module	
	12.1(8a)EWSupport forThis command is not supportedThe bandwidth and shape ratesThe bandwidth can be configureUplink ports on SupervisoPorts on the WS-X4306-GThe two 1000BASE-X porThe first two ports on the YThe two 1000BASE-X por	this command was introduced on the Catalyst 4500 series switch d on the Supervisor Engine 6-E and Catalyst 4900M chassis. s cannot exceed the maximum speed of the interface. red only on the following: r Engine III (WS-X4014) B module ts on the WS-X4232-GB-RJ module	
ExamplesThis example shows how to allocate bandwidth on queue 1 to 100 Mbps:
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] 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] Switch(config-if)# tx-queue]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]Switch(config-if)# tx-queue]Switch(config-if)=tx-queue]Switch(config-if)=tx-queue]Switch(config-if)=tx-queue]Switch(config-if)=tx-queue]Switch(config-if)=tx-queue]Switch(config-if)=tx-queue]Switch(config-if)=tx-queue]Switch(config-if-tx-queue)=Switch(config-if-tx-queue)=Switch(config-if-tx-queue)=Switch(config-if-tx-queue)=Switch(config-if-tx-queue)=

Related Commands	Command	Description
	show qos interface	Displays queueing information.

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 this command to do the following:

- Disable normal mode UDLD on all the fiber ports by default
- Disable aggressive mode UDLD on all the 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 the fiber interfaces.	
	aggressive		Enables UDLD in aggressive mode by default on all the fiber interfaces.	
	message time <i>n</i>	nessage-timer-time	Sets the period of time between the UDLD probe messages on the ports that are in advertisement mode and are currently determined to be bidirectional; valid values are from 1 to 90 seconds.	
Defaults	All fiber interfac	es are disabled and	the message timer time equals 15 seconds.	
Command Modes	Global configura	ation mode		
Command History	Release	Modification		
	12.1(8a)EW	Support for this c	ommand was introduced on the Catalyst 4500 series switch	
Usage Guidelines	or in the detectio	n phase, UDLD resta	all the neighbors of a port have aged out either in the advertisement arts the linkup sequence to try to resynchronize with any potentially in the port if the message train from the link is still undetermined.	
		ffects the fiber interf on the other interfa	faces only. Use the udld (interface configuration mode) command ce types.	
Examples	This example sh	ows how to enable U	JDLD on all the fiber interfaces:	

Related Commands	Command	Description
	show udld	Displays the administrative and operational UDLD status.
	udld (interface configuration	Enables UDLD on an individual interface or prevents a fiber
	mode)	interface from being enabled by the udld (global configuration
		mode) command.

udld (interface configuration mode)

To enable UDLD on an individual interface or to prevent a fiber interface from being enabled by the **udld** (global configuration mode) command, use the **udld** command. To return to the **udld** (global configuration mode) command setting, or if the port is a nonfiber port to disable UDLD, use the **no** form of this command.

udld {enable | aggressive | disable}

no udld {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 udld (enable or aggressive) command, the nonfiber interfaces are enabled with UDLD disabled.		
Command Modes	Interface conf	iguration mode	
Command History	Release	Modification	
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.	
Usage Guidelines	or in the detec	aggressive mode, once all the neighbors of a port have aged out either in the advertisement tion phase, UDLD restarts the linkup sequence to try to resynchronize with any potentially eighbor and shuts down the port if the message train from the link is still undetermined.	
	Use the no udld enable command on the fiber ports to return control of UDLD to the global udld enable command or to disable UDLD on the nonfiber ports.		
	Use the udld aggressive command on the fiber ports to override the setting of the global aggressive) command. Use the no form on the fiber ports to remove this setting, return cor enabling back to the global udld command or to disable UDLD on the nonfiber ports.		
	The disable keyword is supported on the fiber ports only. Use the no form of this command to remove this setting and return control of UDLD to the udld (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 **udld** (global configuration mode) setting:

Switch (config-if)# udld 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	Command	Description
	show udld	Displays the administrative and operational UDLD status.
	udld (global configuration	Enables aggressive or normal mode in the UDLD protocol and sets
	mode)	the configurable message timer time.

udld reset

To reset all the 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 mode

 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 the 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 the ports that are shut down by UDLD: Switch# udld reset Switch#

Related Commands	Command	Description
	show udld	Displays the administrative and operational UDLD status.

unidirectional

To configure the 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 the u	nidirectional reception.	
	send-only	Specifies the u	nidirectional transmission.	
Defaults	Disabled			
Command Modes	Interface config	guration mode		
Command History	Release	Modification		
oominana motory				
		unidirectional mo	de automatically disables port UDLD. You must manually ensure that create a spanning-tree loop in the network.	
Usage Guidelines	Enabling port ut the unidirection	inidirectional mo nal link does not	de automatically disables port UDLD. You must manually ensure that create a spanning-tree loop in the network.	
Usage Guidelines Examples	Enabling port u the unidirection This example s Switch# confi Enter configu Switch(config	nidirectional mo nal link does not hows how to set g terminal ration commands)# interface gi -if)# unidirect	de automatically disables port UDLD. You must manually ensure that	
Usage Guidelines	Enabling port u the unidirection This example s Switch# confi Enter configu Switch(config Switch(config Switch(config	nidirectional mo nal link does not hows how to set g terminal ration commands)# interface gi -if)# unidirect	de automatically disables port UDLD. You must manually ensure that create a spanning-tree loop in the network. Gigabit Ethernet interface 1/1 to receive traffic unidirectionally: , one per line. End with CNTL/Z. gabitethernet 1/1	

username

To establish a username-based authentication system, use the username command.

username *name* **secret** {**0** | **5**} *password*

name secret 0 5 password No username-ba	User ID of the user. 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). Password of the user.	
password	immediately following is not encrypted) and 5 (text immediately following is encrypted using an MD5-type encryption method). Password of the user.	
<u></u>		
No username-ba		
	sed authentication system is established.	
Global configura	ation mode	
Release	Modification	
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.	
enables MD5 en retrievable. You CHAP.	nd to enable enhanced password security for the specified username. This command cryption on the password. MD5 encryption is a strong encryption method that is not cannot use MD5 encryption with protocols that require clear-text passwords, such as	
	username that does not require a password but that connects the user to a information service.	
The username command provides both username and secret authentication for login purposes only		
The <i>name</i> argument can be only one word. White spaces and quotation marks are not allowed.		
You can use mul	tiple username commands to specify options for a single user.	
For information	about additional username commands, refer to the Cisco IOS Command Reference.	
This example sh	ows how to specify an MD5 encryption on a password (warrior) for a username (xena):	
	# username xena secret 5 warrior #	
	Release12.1(8a)EWUse this command enables MD5 en retrievable. You CHAP.You can use this define an "info" general-purpose The username of The name argum You can use mul For informationThis example sh	

Related Commands	Command	Description
	enable password (refer to Cisco IOS documentation)	Sets a local password to control access to various privilege levels.
	enable secret (refer to Cisco IOS documentation)	Specifies an additional layer of security over the enable password command.
	username (refer to Cisco IOS documentation)	Establishes a username-based authentication system.

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 the MD5 signatures.	
	flash-filesystem:	(Optional) Device where the Flash resides; valid values are bootflash :, slot0: , flash: , or sup-bootflash: .	
	filename	(Optional) Name of the Cisco IOS image.	
	expected-md5-signature	(Optional) MD5 signature.	
Defaults	The current working device is specified.		
Command Modes	Privileged EXEC mode		
Command History	Release Modific	cation	
	12.1(8a)EW Suppor	t for this command was introduced on the Catalyst 4500 series switch	
Usage Guidelines	e	is distributed on the disk uses a single checksum for the entire image. This ly when the image is copied into the Flash memory.	
	of the image. Review the c	s included with the image on the disk, lists the name, file size, and checksum contents of the Readme file before loading or duplicating the new image so that um when you copy it into the Flash memory or on to a server.	
	validates the integrity of a	mand to verify the MD5 signature of a file before using it. This command a copied file by comparing a precomputed MD5 signature with the signature ommand. If the two MD5 signatures match, the copied file is identical to the	
	You can find the MD5 signature posted on the Cisco.com page with the image.		
	You can use the verify /m	d5 command in one of the following ways:	
	• Verify the MD5 signa	tures manually by entering the verify /md5 <i>filename</i> command.	
	Check the displayed s	signature against the MD5 signature posted on the Cisco.com page.	
		compare the MD5 signatures by entering the verify /md5	

• 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:

To display the contents of the Flash memory, enter the **show flash** command. The Flash contents listing does not include the checksum of the individual files. To recompute and verify the image checksum after the image has been copied into the Flash memory, enter the **verify** command.

A colon (:) is required after the specified device.

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 verify the MD5 signature:

```
Switch# verify /md5 c4-jsv-mz
```

This example shows how to allow the system to compare the MD5 signatures:

Switch# verify /md5 slot0:c4-jsv-mz 0f369ed9e98756f179d4f29d6e7755d3

Related Commands	Command	Description
	show file system (Flash file system) (refer to Cisco IOS documentation)	Displays available file systems.
	show flash (refer to Cisco IOS documentation)	Displays the contents of flash memory.

Examples

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] [backupcrf mode] [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	vlan_id	Number of the VLAN; valid values are from 1 to 4094.
	are hops	(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.
	backupcrf mode	(Optional) Enables or disables the backup CRF mode of the VLAN; valid values are enable and disable .
	bridge type	(Optional) Specifies the bridging characteristics of the VLAN or identification number of the bridge; valid <i>type</i> values are srb and srt .
	bridge_num	(Optional) Valid bridge_num values are from 0 to 15.
	media type	(Optional) Specifies the media type of the VLAN; valid values are fast ethernet, fd-net, fddi, trcrf, and trbrf.
	mtu mtu-size	(Optional) Specifies the maximum transmission unit (packet size, in bytes) that the VLAN can use; valid values are from 576 to 18190.
	name vlan-name	(Optional) Defines a text string used as the name of the VLAN (1 to 32 characters).
	parent parent-vlan-id	(Optional) Specifies the ID number of the parent VLAN of FDDI or Token Ring-type VLANs; valid values are from 2 to 1001.
	ring ring-number	(Optional) Specifies the ring number of FDDI or Token Ring-type VLANs; valid values are from 2 to 1001.
	said said-value	(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 type	(Optional) Specifies the STP type; valid values are ieee, ibm, and auto.
	tb-vlan1 tb-vlan1-id	(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 tb-vlan2-id	(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 mode				
Command Modes	VLAN configuration mode Release Modification				
	Release Modification				
Command History	ReleaseModification12.1(8a)EWSupport for this command was introduced on the Catalyst 4500 series switch				
Command History	Release Modification 12.1(8a)EW Support for this command was introduced on the Catalyst 4500 series switch VLAN 1 parameters are factory configured and cannot be changed.				
Command History	Release Modification 12.1(8a)EW Support for this command was introduced on the Catalyst 4500 series switch 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				
Command History	Release Modification 12.1(8a)EW Support for this command was introduced on the Catalyst 4500 series switch 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.				
Command History	Release Modification 12.1(8a)EW Support for this command was introduced on the Catalyst 4500 series switch 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				
Command History	Release Modification 12.1(8a)EW Support for this command was introduced on the Catalyst 4500 series switch 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				

Examples

This example shows how to add a new VLAN with all the default parameters to the new VLAN database: Switch(vlan)# vlan 2



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 the 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	Command	Description
	show vlan	Displays VLAN information.

OL-16005-01

vlan access-map

To enter 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	name	VLAN access-map tag.	
	seq#	(Optional) Map sequence number; valid values are from 0 to 65535.	
Defaults	This command I	has no default settings.	
Command Modes	Global configur	ation mode	
Command History	Release	Modification	
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch	
Usage Guidelines	you do not spec clause and one a command witho access-map moo	sequence number of an existing map sequence, you enter VLAN access-map mode. If ify a sequence number, a number is automatically assigned. You can enter one match action clause per map sequence. If you enter the no vlan access-map name [<i>seq#</i>] out entering a sequence number, the whole map is removed. Once you enter VLAN de, the following commands are available: ts 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 sh	nows how to enter VLAN access-map mode:	
	Switch(config) Switch(config-	# vlan access-map cisco access-map)#	

Related Commands	Command	Description
	match	Specifies a match clause by selecting one or more ACLs for a VLAN access-map sequence.
	show vlan access-map	Displays the contents of a VLAN access map.

vlan configuration

To configure a service-policy on a VLAN, use the **vlan configuration** command to enter the VLAN feature configuration mode.

vlan configuration {vlan}

Syntax Description	vlan	Specifies a list of VLANs. "," "-" operators can be used; such as, 1-10,20.
Defaults	This command	has no default settings.
Command Modes	Configuration	mode
Command History	Release	Modification
	12.2(40)SG	This command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6E.
Usage Guidelines	Configuring of 4900M chassis	f service-policies in this mode is supported on the Supervisor Engine 6-E and Catalyst s.
		Engines V through 10GE and earlier, a service-policy has to attach to SVI to apply policies. Even though an SVI is not needed in all cases, such as when you use your Catalyst itch as a pure Layer 2 switch, you are required to create an SVI.
	Supervisor Eng and the input a requirement fo	requirement of creating an SVI, VLAN configuration mode is introduced on the gine 6-E and Catalyst 4900M chassis. With this command you can specify lists of VLANs and output policies that are applied. To configure your system in this mode there is no or you to create SVIs, or create VLAN or VTP mode interactions. Once the VLAN e the configuration becomes active on that VLAN. You can use "-" or "," extensions to AN list.
Examples	This example s the new service	shows how to configure a service policy while in VLAN configuration mode and display e policy:
	Switch(config Switch(config	gure terminal g)#vlan configuration 30-40 g-vlan-config)#service-policy input p1 g-vlan-config)#end cunning configuration begin vlan configuration
	vlan configur service-po !	ration 30-40 Dlicy input p1 . allocation policy ascending !
	! Switch#	

This example shows how to display the new service policy:

```
Switch#show policy-map vlan 30
vlan 30
Service-policy input: p1
Class-map: class-default (match-any)
0 packets
Match: any
0 packets
police:
    rate 128000 bps, burst 4000 bytes
    conformed 0 packets, 0 bytes; action:
        transmit
        exceeded 0 packets, 0 bytes; action:
            drop
            conformed 0 bps, exceeded 0 bps
Switch#
```

Related Commands	Command	Description
	vlan (VLAN Database mode)	Configures a specific VLAN.
	policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.

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 mode

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 the current changes and bumps the revision number.
- exit—Applies the 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 the current changes and rereads the current database.
- **show**—Displays the database information.
- **vlan**—Accesses the 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 the 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#

Catalyst 4500 Series Switch Cisco IOS Command Reference—Release 12.2(46)SG

Γ

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	Command	Description
	show vlan	Displays VLAN information.

vlan dot1q tag native

To enable tagging of the native VLAN frames on all 802.1Q trunk ports, use the **vlan dot1q tag native command.** To disable tagging of native VLAN frames, use the **no** form of this command.

vlan dot1q tag native

no vlan dot1q tag native

Defaults 802.1Q native VLAN tagging is d
--

Command Modes Global configuration mode

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

Usage Guidelines When enabled, the native VLAN packets exiting all 802.1Q trunk ports are tagged unless the port is explicitly configured to disable native VLAN tagging.

When disabled, the native VLAN packets exiting all 802.1Q trunk ports are not tagged.

You can use this command with 802.1Q tunneling. 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 the 802.1Q trunk ports for sending out the packets to the service-provider network. However, the packets going through the core of the service-provider network might also be carried on the 802.1Q trunks. If the native VLANs of an 802.1Q trunk match the native VLAN of a tunneling port on the same switch, the traffic on the native VLAN is not tagged on the sending trunk port. This command ensures that the native VLAN packets on all 802.1Q trunk ports are tagged.

Examples

This example shows how to enable 802.1Q tagging on the native VLAN frames and verify the configuration:

Switch# config terminal Switch (config)# vlan dotlq tag native Switch (config)# end Switch# show vlan dotlq tag native dotlq native vlan tagging is enabled

Γ

Related Commands	Command	Description
	switchport private-vlan trunk native vlan tag	Configures the tagging of the native VLAN traffic on 802.1Q private VLAN trunks.
	switchport trunk	Sets the trunk characteristics when an interface is in trunking mode.

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	map-name	VLAN access-map tag.	
- ,	vlan-list vlan-lis		
Defaults	This command h	as no default settings.	
Command Modes	Global configuration mode		
Command History	Release	Modification	
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch	
Usage Guidelines	• You can app	g an action clause in a VLAN access map, note the following: ly the VLAN access map to one or more VLANs.	
		<i>t</i> parameter can be a single VLAN ID, a list of VLAN IDs, or VLAN ID ranges <i>n-id</i>). Multiple entries are separated by (-), (hyphen), or (,) (comma).	
	• You can app	ly only one VLAN access map to each VLAN.	
	vlan-list is requi	ne no form of this command, the <i>vlan-list</i> parameter is optional (but the keyword red). If you do not enter the <i>vlan-list</i> parameter, the VACL is removed from all the map-name is applied.	
Examples	This example sho	ows how to apply a VLAN access map on VLANs 7 through 9:	
	Switch(config)# Switch(config)#	vlan filter ganymede vlan-list 7-9	

vlan internal allocation policy

To configure the internal VLAN allocation scheme, use the **vlan internal allocation policy** command. To return to the default setting, use the **no** form of this command.

vlan internal allocation policy {ascending | descending}

no vlan internal allocation policy

Syntax Description	ascending Specifies to allocate internal VLANs from 1006 to 4094.				
	descending	Specifies to allocate internal VLANs from 4094 to 1006.			
Defaults	The default is the ascending allocation scheme.				
Command Modes	Global configuration mode				
Command History	History Release Modification				
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch			
Usage Guidelines	You can config	ure internal VLAN allocation to be from 1006 and up or from 4094 and down.			
	The 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.				
	allocated first. ' configure a VL	bootup, the internal VLANs that are required for features in the startup-config file are The user-configured VLANs in the startup-config file are configured next. If you AN that conflicts with an existing internal VLAN, the VLAN that you configured is put ational status until the internal VLAN is freed and becomes available.			
	After you enter used by the por	the write mem command and the system reloads, the reconfigured allocation scheme is t manager.			
Examples	This example shows how to configure the VLANs in a descending order as the internal VLAN allocation policy:				
	Switch(config Switch(config)# vlan internal allocation policy descending)#			
Related Commands	Command	Description			
	show vlan inte	•			

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	interval	Queries to the VLAN Membership Policy Server (VMPS) to reconfirm dynamic VLAN assignments; valid values are from 1 to 120 minutes.	
Defaults	The reconfirmation	on interval is 60 minutes.	
ommand Modes	Global configuration mode		
Command History	Release	Modification	
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch	
xamples	Switch(config)#	ows how to set the VQP client to reconfirm dynamic VLAN entries every 20 minutes vmps reconfirm 20	
Examples	Switch(config)# Switch(config)#	vmps reconfirm 20	
xamples Related Commands	Switch(config)# Switch(config)# You can verify yo	vmps reconfirm 20 bur setting by entering the show vmps command and examining information in the	
	Switch(config)# Switch(config)# You can verify yo Reconfirm Interva	vmps reconfirm 20 bur setting by entering the show vmps command and examining information in the al row.	

vmps reconfirm (privileged EXEC)

To immediately send VLAN Query Protocol (VQP) queries to reconfirm all the dynamic VLAN assignments with the VLAN Membership Policy Server (VMPS), use the **vmps reconfirm** command.

vmps reconfirm

Syntax Description	This command	has no argumen	ts or keywords.
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 Catalyst 4500 series switch
Usage Guidelines	of the Reconfirm	nation Status see re reconfirmed	entering the show vmps command and examining the VMPS Action row ction. The show vmps command shows the result of the last time that the either because the reconfirmation timer expired or because the vmps ed.
Examples	This example sl Switch# vmps r Switch#		mediately send VQP queries to the VMPS:
Related Commands	Command		Description
	show vmps		Displays the VLAN Query Protocol (VQP) version, reconfirmation interval, retry count, VLAN Membership Policy Server (VMPS) IP addresses, current servers, and primary servers.
	vmps reconfir configuration)		Changes the reconfirmation interval for the VLAN Query Protocol (VQP) client.

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	count	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 coun	t is 3.
Command Modes	Global configu	ration mode
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 Server Retry C	your setting by entering the show vmps command and examining information in the count row.
Examples	×.	shows how to set the retry count to 7:
Related Commands	Command	Description
	show vmps	Displays the VLAN Query Protocol (VQP) version, reconfirmation interval, retry count, VLAN Membership Policy Server (VMPS) IP addresses, current servers, and primary servers.

vmps server

To configure the primary VLAN Membership Policy Server (VMPS) and up to three secondary servers, use the **vmps server** command. To remove a VMPS server, use the **no** form of this command.

vmps server ipaddress [primary]

no vmps server ipaddress

Syntax Description	<i>ipaddress</i> IP address or host name of the primary or secondary VMPS servers. If you spear a hostname, the Domain Name System (DNS) server must be configured.			
	primary	(Optional) Determines whether primary or secondary VMPS servers are being configured.		
Defaults	No primary or secondary VMPS servers are defined.			
Command Modes	Global configuration mode			
Command History	Release	Modification		
	12.1(4)EA1	Support for this command was introduced on the Catalyst 4500 series switch		
Usage Guidelines	The first server that you 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.			
	delete all server	e no form without specifying the <i>ipaddress</i> , all configured servers are deleted. If you as when dynamic-access ports are present, the switch cannot forward the packets from the these ports because it cannot query the VMPS.		
	You can verify VMPS Domain	your setting by entering the show vmps command and examining information in the 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	Command	Description
	show vmps	Displays the VLAN Query Protocol (VQP) version,
		reconfirmation interval, retry count, VLAN Membership Policy
		Server (VMPS) IP addresses, current servers, and primary
		servers.

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 <i>name</i> is an ASCII string limited to 255 characters.
Defaults	Disabled	
Command Modes	Global configu	ration mode
Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch
Usage Guidelines	which the exist You can use the	the vtp file command to load a new database. You can use it only to rename the file in ing database is stored. e vtp if-id command to specify the name of the interface providing the VTP updater ID
		The VTP updater is the device that adds, deletes, or modifies VLANs to a network, and updater to inform the rest of the system of the changes.
Examples	This example s	hows how to specify the IFS file system file where VTP configuration is stored:
)# vtp file vtpconfig e to store VLAN database at filename vtpconfig.)#
	This example s	hows how to specify the name of the interface providing the VTP updater ID:
	Switch(config Switch(config)# vtp if-id fastethernet)#
Related Commands	Command	Description
	show vtp	Displays VTP statistics and domain information.

vtp client

To place a device in VTP client mode, use the **vtp client** command. To return to VTP server mode, use the **no** form of this command.

vtp client

no vtp client

Defaults Disabled

Command Modes VLAN configuration mode

 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	Command	Description
	show vtp	Displays VTP statistics and domain information.
	vtp (global configuration mode)	Configures the name of a VTP configuration storage file.

vtp domain

To configure the administrative domain name for a device, use the vtp domain command.

vtp domain domain-name

Syntax Description	domain-name	Name of the domain.	
Defaults	This command h	as no default settings.	
Command Modes	VLAN configuration mode		
Command History	Release	Modification	
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch	
Usage Guidelines	You must set a d Even if you do n	e the <i>domain-name</i> , the domain name is case sensitive and can be from 1 to 32 characters. Iomain name before you can transmit any VTP advertisements. Not set a domain name, the device will leave the no-management-domain state upon st VTP summary packet on any port that is currently trunking.	
	If the device rec zero. Once the d	eives its domain from a summary packet, it resets its configuration revision number to evice leaves the no-management-domain state, it can never be configured to reenter the by cleaning NVRAM and reloading.	
Examples	-	ows how to set the devices administrative domain: nfig)# vtp domain DomainChandon nfig)#	
Related Commands	Command	Description	
	show vtp	Displays VTP statistics and domain information.	

vtp (global configuration mode)	Configures the name of a VTP configuration storage file.
---------------------------------	--

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 Defaults Command Modes	password-value	An ASCII string, from 1 to 32 characters, identifying the administrative domain for the device.			
	Disabled				
	VLAN configuration mode				
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	Command	Description			
	show vtp	Displays VTP statistics and domain information.			
	vtp (global confi mode)	guration Configures the name of a VTP configuration storage file.			

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 mode

 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	Command	Description
	show vtp	Displays VTP statistics and domain information.
	vtp (global configuration mode)	Configures the name of a VTP configuration storage file.

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 mode

 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)#

Commands Command Description show vtp Displays VTP statistics and domain information. vtp (global configuration mode) Configures the name of a VTP configuration storage file.

Γ

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 mode

 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. The 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	Command	Description
	show vtp	Displays VTP statistics and domain information.
	vtp (global configuration mode)	Configures the name of a VTP configuration storage file.
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 mode

 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 version 2 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, the 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	Command	Description
	show vtp	Displays VTP statistics and domain information.
	vtp (global configuration mode)	Configures the name of a VTP configuration storage file.

vtp v2-mode





Abbreviations

Α

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

В

BEM	best effort method
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
СНАР	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 Rotuing Protocol
DXI	data exchange interface

Ε

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
ISSU	In Service Software Upgrade

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

Μ	_
MAC	Media Access Control
MCL	Mismatched Command List
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
МОР	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

Ν

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

0

OAM	Operation, Administration, and Maintenance
OSI	Open System Interconnection
OSPF	open shortest path first

Ρ

PAE	port access entity
PAgP	Port Aggregation Protocol
PBD	packet buffer daughterboard
PC	Personal Computer (formerly PCMCIA)
РСМ	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
РНҮ	physical sublayer
PIB	policy information base
PIM	Protocol Independent Multicast
PM	Port manager

PPP	Point-to-Point Protocol

PRC	Parser Return Code

- 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

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

Т

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

Χ

XNS Xerox Network System



Symbols

\$ matches the end of a string 1-7
() in commands 1-11
* 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

10-Gigabit Ethernet uplink selecting 2-151 showing the mode 2-455, 2-456 802.1Q trunk ports and native VLANs 2-778 802.1Q tunnel ports configuring 2-720 802.1S Multiple Spanning Tree see MST 802.1X configuring for multiple hosts 2-119 configuring for single host 2-119 configuring multiple domains 2-119 disabling port control 2-112 enabling port control 2-112 802.1X Critical Authentication disabling on a port 2-113 disabling on a VLAN 2-116

ΙΝΟΕΧ

EAPOL

disabling send success packets 2-114 enabling send success packets 2-114 enabling on a port 2-113 enabling on a VLAN 2-116 returning delay time to default setting 2-115 setting delay time on a port 2-115 802.1X Port Based Authentication debugging 802.1X Port Based Authentication 2-74 displaying port based authentication 2-439 enabling accounting for authentication sessions 2-4 enabling authentication on the system 2-130 enabling guest VLAN 2-117 enabling guest VLAN supplicant 2-110, 2-118 enabling manual control of auth state 2-126 enabling periodic re-authentication of the client 2-129 initializing re-authentication of dot1x ports 2-128 initializing state machines 2-121 receive session termination message upon reboot 2-5 setting maximum number for EAP requests 2-124 setting the reauthentication timer 2-131

A

abbreviating commands context-sensitive help 1-1 Access Gateway Module connecting to a module 2-17 connecting to a remote module 2-380 connecting to a specific remote module 2-392 access-group displaying mac interface 2-560 show mode interface 2-411 access groups IP 2-6 access lists clearing an access template 2-39 defining ARP 2-16 displaying ARP information 2-414 See also ACLs, MAC ACLs, and VACLs access maps applying with VLAN filter 2-780 ACLs access-group mode 2-6 balancing hardware regions 2-12 capturing control packets 2-8 determining ACL hardware programming 2-10 disabling hardware statistics 2-146 displaying mac access-group interface 2-560 enabling hardware statisctics 2-146 using ACL naming conventions for MAC ACLs 2-258 action clause specifying drop or forward action in a VACL 2-13 addresses, configuring a maximum 2-335 adjacency debugging the adjacency table 2-67 disabling the debug facility 2-67 displaying information about the adjacency table **2-412** displaying IPC table entries 2-67 aggregate policer displaying information 2-612 aging time displaying MAC address aging time 2-563 MAC address table 2-261 alarms displaying operational status 2-443

alternation description 1-10 anchoring description 1-10 ARP access list, displaying detailed information 2-414 defining access-lists 2-16 **ARP** inspection enforce certain types of checking 2-168 ARP packet deny based on DHCP bindings 2-106 permit based on DHCP bindings 2-308 authentication setting username 2-765 using an MD5-type encryption method 2-765 verifying MD5 signature 2-767 verifying the checksum for Flash memory 2-767 auth fail VLAN enable on a port 2-111 set max number of attempts 2-110 authorization state enabling manual control 2-126 authorization state of a controlled port 2-126 automatic installation displaying status 2-415 automatic medium-dependent interface crossover See Auto-MDIX Auto-MDIX disabling 2-290 enabling 2-290 auto-negotiate interface speed example 2-709 auto-QoS configuring for VoIP 2-18 displaying configuration 2-416

В

baby giants displaying the system MTU setting 2-643 setting the maximum Layer 2 payload size 2-745 BackboneFast displaying debugging messages 2-93 displaying spanning tree status 2-633 enabling debugging 2-93 bandwidth command 2-22 bindings store for DHCP snooping 2-180 BOOT environment variable displaying information 2-419 bootflash displaying information 2-417 **BPDUs** debugging spanning tree activities 2-91 bridge protocol data units See BPDUs broadcast counters 2-64 broadcast suppression level configuring **2-710**, **2-712** enabling 2-710, 2-712

С

cable diagnostics TDR displaying test results 2-420 testing conditions of copper cables 2-747 Catalyst 4507R 2-331 CDP configuring tunneling encapsulation rate 2-248 displaying neighbor information 2-422 enabling protocol tunneling for 2-243 set drop threshold for 2-246

CEF displaying next-hop information 2-492 displaying VLAN configuration information 2-492 cisco-desktop macro apply 2-268 Cisco Express Forwarding See CEF cisco-phone macro apply 2-270 cisco-router macro apply 2-272 cisco-switch macro apply 2-274 class maps creating 2-32 defining the match criteria 2-283 clear commands clearing Gigabit Ethernet interfaces 2-37 clearing IGMP group cache entries 2-46 clearing interface counters 2-34 clearing IP access lists 2-39, 2-40 clearing IP ARP inspection statistics VLAN 2-41 clearing IP DHCP snooping database statistics 2-45 clearing MFIB counters and routes 2-49 clearing MFIB fastdrop entries 2-50 clearing PAgP channel information 2-55 clearing QoS aggregate counters 2-58 clearing VLAN interfaces 2-38 CLI string search anchoring 1-10 expressions 1-7 filtering 1-6 multiple-character patterns 1-8 multipliers 1-9 parentheses for recall 1-11 searching outputs 1-6 single-character patterns 1-7 using 1-6

command modes accessing privileged EXEC mode 1-5 exiting 1-5 understanding user EXEC and configuration modes 1-5 condition interface debugging interface-related activities 2-69 condition vlan debugging VLAN output 2-72 configuration, saving 1-11 configuring root as secondary 2-693 configuring a SPAN session to monitor limit SPAN source traffic 2-295 configuring forward delay 2-689 configuring root as primary 2-693 CoPP attaching policy map to control plane 2-390 displaying policy-map class information 2-589 entering configuration mode 2-62 removing service policy from control plane 2-390 CoS assigning to Layer 2 protocol packets 2-245 CoS QoS default defining value on an interface 2-356 Cost of Service See QoS CoS counters clearing interface counters 2-34

D

DAI

clear statistics 2-41

DBL displaying qos dbl 2-613 enabling DBL globally on the switch 2-357 debug commands debugging backup events 2-68 debugging DHCP snooping events 2-79 debugging DHCP snooping messages 2-80 debugging EtherChannel/PAgP/shim 2-75 debugging IPC activity 2-78 debugging IP DHCP snooping security messages 2-81 debugging NVRAM activities 2-84 debugging PAgP activities 2-85 debugging port manager activities 2-88 debugging spanning tree activities 2-91 debugging spanning tree backbonefast 2-93 debugging spanning tree UplinkFast 2-96 debugging supervisor redundancy 2-90 debugging VLAN manager activities 2-97 displaying monitor activity 2-83 displaying the adjacency table 2-67 enabling debug dot1x 2-74 enabling debugging messages for ISL VLAN IDs 2-100 enabling debugging messages for VTP 2-101 enabling debugging of UDLD activity 2-102 enabling switch shim debugging 2-94 enabling VLAN manager file system error tests 2-98 limiting debugging output for VLANs 2-72 limiting interface debugging output 2-69 limiting output for debugging standby state changes 2-70 shortcut to the debug condition interface 2-77 debugging activity monitoring 2-83 DHCP snooping events 2-79 DHCP snooping packets 2-80 IPC activities 2-78 IP DHCP snooping security packets 2-81

NVRAM activities 2-84

PAgP activities 2-85 PAgP shim 2-75 PM activities 2-88 spanning tree BackboneFast events 2-93 spanning tree switch shim 2-94 spanning tree UplinkFast events 2-96 VLAN manager activities 2-97 VLAN manager IOS file system error tests 2-98 VTP protocol debug messages 2-101 debug spanning tree switch 2-94 debug sw-vlan vtp 2-101 default CoS value 2-356 default form of a command, using 1-6 defining egress DSCP-to-CoS mapping 2-363 DHCP clearing database statistics 2-45 **DHCP** bindings configuring bindings 2-178 deny ARP packet based on matches 2-106 permit ARP packet based on matches 2-308 DHCP snooping clearing binding entries 2-42 clearing database 2-44 displaying binding table 2-495 displaying configuration information 2-493 displaying status of DHCP database 2-498 displaying status of error detection 2-446 enabling DHCP globally 2-177 enabling IP source guard 2-217 enabling on a VLAN 2-187 enabling option 82 2-182, 2-184 enabling option-82 2-189 enabling rate limiting on an interface 2-185 enabling trust on an interface 2-186 establishing binding configuration 2-178 renew binding database 2-382 store generated bindings 2-180

diagnostic test bootup packet memory 2-433 displaying attributes 2-427 display module-based results 2-429 running 2-109 show results for TDR 2-420 testing conditions of copper cables 2-747 displaying error disable recovery 2-447 displaying inline power status 2-604 displaying monitoring activity 2-83 displaying SEEPROM information GBIC 2-457 displaying SPAN session information 2-642, 2-711 document conventions 1-xviii document organization 1-xvii DoS CoPP attaching policy map to control plane 2-390 displaying policy-map class information 2-589 entering configuration mode **2-62** removing service policy from control plane 2-390 entering CoPP configuration mode 2-62 DOS attack protecting system's resources 2-163 drop threshold, Layer 2 protocol tunneling 2-246 DSCP rewrite for IP packets enable 2-367 dual-capable port selecting a connector 2-292 duplex mode configuring autonegotiation on an interface 2-133 configuring full duplex on an interface 2-133 configuring half duplex on an interface 2-133 dynamic ARP inspection preventing 2-163 Dynamic Buffer Limiting See DBL

Dynamic Host Configuration Protocol See DHCP

Ε

EAP restarting authentication process 2-124 EIGRP (Enhanced IGRP) filters routing updates, preventing 2-305 enabling debugging for UDLD 2-102 voice VLANs 2-713 environmental alarms 2-443 displaying information 2-443 status 2-443 temperature 2-443 erase a file 2-135 error disable detection enabling error disable detection 2-138 error-disabled state displaying 2-476 error disable recovery configuring recovery mechanism variables 2-140 displaying recovery timer information 2-447 enabling ARP inspection timeout 2-140 specifying recovery cause 2-140 EtherChannel assigning interfaces to EtherChannel groups 2-25 debugging EtherChannel 2-75 debugging PAgP shim 2-75 debugging spanning tree activities 2-91 displaying information for a channel 2-449 removing interfaces from EtherChannel groups 2-25 EtherChannel guard detecting STP misconfiguration 2-679

Explicit Host Tracking clearing the database 2-48 enabling per-VLAN 2-201 expressions matching multiple expression occurrences 1-9 multiple-character patterns 1-8 multiplying pattern occurrence 1-11 single-character patterns 1-7 Extensible Authentication Protocol See EAP

F

field replaceable unit (FRU) displaying status information 2-443 filters EIGRP routing updates, preventing 2-305 Flash memory file system displaying file system information 2-417 verifying checksum 2-767 flow control configuring a gigabit interface for pause frames 2-143 displaying per-interface statistics for flow control 2-453

G

GBIC

displaying SEEPROM information 2-457 Gigabit Ethernet interface clearing the hardware logic 2-37 Gigabit Ethernet uplink selecting 2-151 showing the mode 2-455, 2-456 global configuration mode using 1-5

Η

hardware module

resetting a module by toggling the power 2-148 hardware statistics disabling 2-146 enabling 2-146 hardware uplink changing the mode 2-149 selecting the mode 2-151 showing the mode 2-455, 2-456 helper addresses, IP 2-513 hot standby protocol debugging 2-70 disabling debugging 2-70 limiting output 2-70

IDPROMs displaying SEEPROM information chassis 2-457 clock module 2-457 fan trays 2-457 module 2-457 mux buffer 2-457 power supplies 2-457 supervisor engine 2-457 ifIndex persistence clearing SNMP ifIndex commands 2-665 compress SNMP ifIndex table format 2-672 disabling globally 2-671 disabling on an interface 2-667 enabling globally 2-671 enabling on an interface 2-667 IGMP applying filters for host joining on Layer 2 interfaces 2-191 clearing IGMP group cache entries 2-46

configuring frequency for IGMP host-query messages 2-194 creating an IGMP profile 2-193 displaying IGMP interface configuration information 2-500 displaying profiles 2-502 setting maximum group numbers 2-192 IGMP profiles displaying 2-502 IGMP snooping clearing the EHT database 2-48 configuring a Layer 2 interface as a group member 2-207 configuring a Layer 2 interface as a multicast router 2-205 configuring a static VLAN interface 2-207 displaying multicast information 2-509 displaying VLAN information 2-503, 2-507, 2-510 enabling 2-196 enabling immediate-leave processing 2-203 enabling on a VLAN 2-200 enabling per-VLAN Explicit Host Tracking 2-201 informs enabling 2-669 inline power displaying inline power status 2-604 In Service Software Upgrade See ISSU inspection log clearing log buffer 2-40 interface displaying suppressed multicast bytes 2-470 interface capabilities displaying 2-466 interface configuration mode summary 1-5 interface link display cable disconnect time 2-473

interfaces configuring dot1q tunnel ports 2-720 creating an interface-range macro 2-105 debugging output of interface related activities 2-69 displaying description 2-472 displaying error-disabled state 2-476 displaying information when tunneling is enabled 2-554 displaying status 2-472 displaying traffic for a specific interface 2-463 entering interface configuration mode 2-155 executing a command on multiple ports in a range 2-158 selecting an interface to configure 2-155 setting a CoS value for Layer 2 packets 2-245 setting drop threshold for Layer 2 packets 2-246 setting the interface type 2-720 interface speed configuring interface speed 2-707 interface transceiver displaying diagnostic data 2-480 internal VLAN allocation configuring 2-781 default setting 2-781 displaying allocation information 2-655 Internet Group Management Protocol See IGMP IP ARP applying ARP ACL to VLAN 2-161 clearing inspection statistics 2-41 clearing status of log buffer 2-40 controlling packet logging 2-172 enabling dynamic inspection 2-170 limit rate of incoming requests 2-163 set per-port config trust state 2-167 showing status of dynamic ARP inspection 2-487 showing status of log buffer 2-490

IP DHCP Snooping See DHCP snooping IP header validation disabling 2-216 enabling 2-216 **IP** interfaces displaying usability status 2-512 **IP** multicast displaying multicast routing table information 2-518 **IP** packets enable DSCP rewrite 2-367 IP phone and standard desktop enabling Cisco-recommended features 2-270 **IP Port Security** enabling 2-217 IP source binding adding or deleting 2-213 displaying bindingstagging 2-523 IP source guard debugging messages 2-81 displaying configuration and filters 2-525 enabling on DHCP snooping 2-217 IPv6 MLD configuring queries 2-223, 2-225 configuring snooping last-listener-query-intervals 2-225 configuring snooping listener-message-suppression 2-227 configuring snooping robustness-variables 2-228 configuring ten topology change notifications 2-230 counting snooping last-listener-queries 2-223 displaying information 2-530 displaying ports for a switch or VLAN 2-532 displaying querier information 2-533 enabling snooping 2-221 enabling snooping on a VLAN 2-231

IPC

debugging IPC activities 2-78

ISSU

canceling process 2-233 configuring rollback timer 2-242 displaying capability 2-535 displaying client information 2-537 displaying compatibility matrix 2-539 displaying endpoint information 2-544 displaying entities 2-545 displaying FSM session 2-546 displaying messages 2-547 displaying negotiated 2-549 displaying rollback-timer 2-550 displaying session information 2-551 displaying software version 2-552 displaying state 2-552 forcing switchover to standby supervisor engine 2-241 loading new image 2-237 starting process 2-239 stopping rollback timer 2-235

J

Jumbo frames enabling jumbo frames **2-301**

L

LACP

deselecting channeling protocol 2-27 enabling LACP on an interface 2-27 setting channeling protocol 2-27 Layer 2 displaying ACL configuration 2-560 Layer 2 interface type specifying a nontrunking, nontagged single VLAN interface 2-720 specifying a trunking VLAN interface 2-720 Layer 2 protocol ports displaying 2-554 Layer 2 protocol tunneling error recovery 2-248 Layer 2 switching enabling voice VLANs 2-713 modifying switching characteristics 2-713 Layer 2 traceroute IP addresses 2-752 Layer 3 switching displaying information about an adjacency table 2-412 displaying port status 2-478 displaying status of native VLAN tagging 2-478 link-status event messages disabling globally 2-252, 2-255 on an interface 2-253, 2-256 enabling globally 2-252, 2-255 on an interface 2-253, 2-256 log buffer show status 2-490 logging controlling IP ARP packets 2-172

Μ

MAC Access Control Lists See MAC ACLs MAC ACLs defining extended MAC access list 2-258 displaying MAC ACL information 2-652 naming an ACL 2-258 MAC address filtering configuring 2-267 disabling 2-267 enabling 2-267

MAC address table adding static entries 2-279 clearing dynamic entries 2-52, 2-54 configuring aging time 2-261 displaying dynamic table entry information 2-567 displaying entry count 2-565 displaying information 2-561 displaying interface-based information 2-569 displaying multicast information 2-571 displaying notification information 2-573 displaying protocol-based information 2-575 displaying static table entry information 2-577 displaying the MAC address aging time 2-563 displaying VLAN-based information 2-580 enabling authentication bypass 2-122 enabling notifications 2-265 learning in the protocol buckets 2-262 removing static entries 2-279 MAC address tables adding static entries 2-267 deleting secure or specific addresses 2-56 disabling IGMP snooping on static MAC addresses 2-267 removing static entries 2-267 mac-address-table static 2-267 MAC address unicast filtering dropping unicast traffic 2-267 macro displaying descriptions 2-278 macro keywords help strings 2-2 macros adding a global description 2-278 cisco global 2-276 system-cpp 2-277 mapping secondary VLANs to MST instance 2-346 mapping VLAN(s) to an MST instance 2-153 match (class-map configuration) command 2-283

maximum transmission unit (MTU) displaying the system MTU setting 2-643 setting the maximum Layer 2 payload size 2-745 MD5 verifying MD5 signature 2-767 message digest 5 See MD5 **MFIB** clearing ip mfib counters 2-49 clearing ip mfib fastdrop 2-50 displaying all active MFIB routes 2-515 displaying MFIB fastdrop table entries 2-517 enabling IP MFIB fastdrops 2-210 MLD configuring snooping last-listener-query-intervals 2-225 configuring snooping listener-message-suppression 2-227 configuring snooping robustness-variables 2-228 configuring topology change notifications 2-230 counting snooping last-listener-queries 2-223 enabling snooping 2-221 enabling snooping on a VLAN 2-231 MLD snooping displaying 2-533 modes access-group 2-6 show access-group interface 2-411 switching between PVST+, MST, and Rapid PVST 2-684 See also command modes module password clearing 2-36 module reset resetting a module by toggling the power 2-148 --More-- prompt filter 1-6 search 1-7

MST

designating the primary and secondary root 2-693
displaying MST protocol information 2-638
displaying region configuration information 2-638
displaying spanning tree information 2-638
entering MST configuration submode 2-687
setting configuration revision number 2-384
setting path cost and port priority for instances 2-685
setting the forward delay timer for all instances 2-689
setting the hello-time delay timer for all instances 2-690
setting the max-age timer for all instances 2-691
setting the MST region name 2-302
specifying the maximum number of hops 2-692
switching between PVST+ and Rapid PVST 2-684
using the MST configuration submode revision command 2-384
using the submode name command 2-302
MTU
displaying global MTU settings 2-643
Multicase Listener Discovery
See MLD
multicast
counters 2-64
enabling storm control 2-712
multicast/unicast packets
prevent forwarding 2-719
Multicast Forwarding Information Base
See MFIB
multiple-character patterns 1-8
Multiple Spanning Tree
See MST

Ν

native VLAN controlling tagging of traffic 2-740 displaying ports eligible for native tagging 2-654 displaying ports eligible for tagging 2-654 enabling tagging on 802.1Q trunk ports 2-778 specifing the tagging of traffic 2-741 NetFlow enabling NetFlow statistics 2-211 including infer fields in routing statistics 2-211 next-hop displaying CEF VLAN information 2-492 no form of a command, using 1-6 NVRAM debugging NVRAM activities 2-84

0

output pattern searches 1-7

Ρ

packet forwarding prevent unknown packets 2-719 packet memory failure direct switch action upon detection 2-108 packet memory test bootup, displaying results 2-433, 2-435 ongoing, displaying results 2-437 PACL access-group mode 2-6 paging prompt see -- More -- prompt PAgP clearing port channel information 2-55 debugging PAgP activity 2-85 deselecting channeling protocol 2-27 displaying port channel information 2-586 hot standby mode returning to defaults 2-304 selecting ports 2-304

input interface of incoming packets learning 2-303 returning to defaults 2-303 setting channeling protocol 2-27 parentheses 1-11 password clearing on an intelligent line module 2-36 establishing enhanced password security 2-765 setting username 2-765 PBR displaying route maps 1-xviii redistributing route maps 1-xviii PM activities debugging 2-88 disabling debugging 2-88 police (percent) command 2-315 police (two rates) command 2-317, 2-319 police command 2-310 Policy Based Routing See PBR policy maps creating 2-323 marking 2-394 See also QoS, hierarchical policies traffic classification defining the class defining trust states 2-755 port, dual-capable selecting the connector 2-292 Port Aggregation Protocol See PAgP port-based authentication displaying debug messages 2-74 displaying statistics and status 2-439 enabling 802.1X 2-126 host modes 2-119 manual control of authorization state 2-126

periodic re-authentication enabling 2-129 re-authenticating 802.1X-enabled ports 2-128 switch-to-client frame-retransmission number 2-124 port channel accessing 2-157 creating 2-157 displaying information 2-586 load distribution method resetting to defaults 2-325 setting 2-325 port range executing 2-158 port security debugging ports security 2-89 deleting secure or specific addresses 2-56 displaying settings for an interface or switch 2-597 enabling 2-725 filter source IP and MAC addresses 2-217 setting action upon security violation 2-725 setting the rate limit for bad packets 2-725 sticky port 2-725 Port Trust Device displaying 2-614 power status displaying inline power 2-604 displaying power status 2-604 power supply configuring combined and redundant power on the Catalyst 4507R 2-331 configuring inline power 2-328 configuring power consumption 2-330 displaying the SEEPROM 2-457 setting inline power state 2-327 priority command 2-337 priority-queue command 2-65 Private VLAN See PVLANs privileged EXEC mode, summary 1-5

prompts system 1-5 protocol tunneling configuring encapsulation rate 2-248 disabling 2-243 displaying port information 2-554 enabling 2-243 setting a CoS value for Layer 2 packets 2-245 setting a drop threshold for Layer 2 packets 2-246 **PVLANs** configuring isolated, primary, and community PVLANs 2-339 controlling tagging of native VLAN traffic 2-740 disabling sticky-ARP 2-214 displaying map information for VLAN SVIs 2-475 displaying PVLAN information 2-657 enabling interface configuration mode 2-720 enabling sticky-ARP 2-214 mapping VLANs to the same SVI 2-343 specifying host ports 2-720 specifying promiscuous ports 2-720 PVST+ switching between PVST and MST 2-684

Q

QoS
account Layer 2 encapsulation 2-349
attaching a policy-map to an interface 2-385
automatic configuration 2-18
class maps
creating 2-32
defining the match criteria 2-283
clearing aggregate counters 2-58
configuring auto 2-18
defining a named aggregate policer 2-351
defining default CoS value 2-356
defining ingress CoS-to-DSCP mapping 2-361
displaying aggregate policer information 2-612

displaying auto configuration 2-416 displaying class maps information 2-425 displaying configuration information 2-416 displaying configurations of policies 2-592 displaying policy map information 2-588, 2-595 displaying QoS information 2-611 displaying QoS map information 2-616 egress queue-sets enabling the priority queue 2-65 enabling global configuration mode 2-347 enabling on control packets 2-354 enabling per-VLAN QoS for a Layer 2 interface 2-370 enabling QoS on an interface 2-348 hierarchical policies average-rate traffic shaping on a class 2-407 bandwidth allocation for a class 2-22, 2-31 creating a service policy 2-388 marking 2-394 strict priority queueing (LLQ) 2-337 mapping DSCP values to transmit queues 2-363 mapping egress DSCP-to-CoS 2-363 mapping the DSCP-to-CoS value 2-363 policy maps creating 2-323 marking 2-394 traffic classifications trust states 2-755 setting the mapping of policed DSCP values 2-365 setting the trust state 2-368 specifying flow-based match criteria 2-286 Supervisor Engine 6-E setting CoS 2-396 setting DSCP 2-399 setting precedence values 2-402 setting QoS group identifiers 2-405

QoS CoS configuring for tunneled Layer 2 protocol packets 2-245 defining default CoS value 2-356 qos dbl 2-357 quality of service See QoS question command 1-1 queueing information displaying 2-614 queue limiting configuring packet limits 2-372

R

Rapid PVST switching between PVST and MST 2-684 re-authenticating 802.1X-enabled ports 2-128 re-authentication periodic 2-129 set the time 2-131 reboots restoring bindings across 2-178 redundancy accessing the main CPU 2-374 changing from active to standby supervisor engine 2-378 displaying information 2-618 displaying ISSU config-sync failure information 2-622 displaying redundancy facility information **2-618** displaying RF client list 2-618 displaying RF operational counters 2-618 displaying RF states 2-618 enabling automatic synchronization 2-21 forcing switchover to standby supervisor engine 2-378 mismatched command listing 2-376 set the mode 2-293

```
synchronizing the route processor
    configurations 2-279
related documentation 1-xvii
remote SPAN
    See RSPAN
renew commands
    ip dhcp snooping database 2-382
resetting PVLAN trunk
    setting switchport to trunk 2-720
rj45 connector, selecting the connector 2-292
ROM monitor mode
    summary 1-6
Route Processor Redundancy
    See redundancy
RPF
    disabling IPv4 exists-only checks 2-219
    enabling IPv4 exists-only checks 2-219
RPR
    set the redundancy mode 2-293
RSPAN
    converting VLAN to RSPAN VLAN 2-381
    displaying list 2-659
```

S

saving configuration changes 1-11 secure address, configuring 2-333 secure ports, limitations 2-726 service-policy command (policy-map class) 2-388 set the redundancy mode 2-293 sfp connector, selecting the connector 2-292 shape command 2-407 show commands filtering parameters 1-7 searching and filtering 1-6 show platform commands 1-11 Simple Network Management Protocol See SNMP single-character patterns special characters 1-7 slaveslot0 displaying information on the standby supervisor 2-629 slot0 displaying information about the system 2-631 **SNMP** debugging spanning tree activities 2-91 ifIndex persistence clearing SNMP ifIndex commands 2-665 compress SNMP ifIndex table format 2-672 disabling globally 2-671 disabling on an interface 2-667 enabling globally 2-671 enabling on an interface 2-667 informs disabling 2-669 enabling 2-669 traps configuring to send when storm occurs 2-710 disabling 2-669 enabling 2-669 mac-notification adding 2-673 removing 2-673 SPAN commands configuring a SPAN session to monitor 2-295 displaying SPAN session information 2-642, 2-711 SPAN enhancements displaying status 2-584 Spanning Tree Protocol See STP SPAN session displaying session information 2-584 filter ACLs 2-295 specify encap type 2-295 turn off host learning based on ingress packets 2-295 special characters anchoring, table 1-10 SSO 2-293 standard desktop enabling Cisco-recommended features 2-268 standard desktop and Cisco IP phone enabling Cisco-recommended features 2-270 sticky address, configuring 2-334 sticky-ARP disabling on PVLANs 2-214 enabling on PVLANs 2-214 sticky port deleting 2-56 enabling security 2-725 storm control configuring for action when storm occurs 2-710 disabling suppression mode 2-446 displaying settings 2-641 enabling 2-710 enabling broadcast 2-710, 2-712 enabling multicast 2-710, 2-712 enabling suppression mode 2-446 enabling timer to recover from error disable 2-140 enabling unicast 2-710, 2-712 multicast, enabling 2-712 setting high and low levels 2-710 setting suppression level 2-446 STP configuring link type for a port 2-682 configuring tunneling encapsulation rate 2-248 debugging all activities 2-91 debugging spanning tree activities 2-91 debugging spanning tree BackboneFast events 2-93 debugging spanning tree UplinkFast 2-96 detecting misconfiguration 2-679 displaying active interfaces only 2-633 displaying BackboneFast status 2-633 displaying bridge status and configuration 2-633 displaying spanning tree debug messages 2-91

Catalyst 4500 Series Switch Cisco IOS Command Reference—Release 12.2(46)SG

displaying summary of interface information 2-633 enabling BPDU filtering by default on all PortFast ports 2-698 enabling BPDU filtering on an interface 2-675 enabling BPDU guard by default on all PortFast ports 2-700 enabling BPDU guard on an interface 2-677 enabling extended system ID 2-680 enabling loop guard as a default on all ports 2-683 enabling PortFast by default on all access ports 2-701 enabling PortFast mode 2-696 enabling protocol tunneling for 2-243 enabling root guard 2-681 enabling spanning tree BackboneFast 2-674 enabling spanning tree on a per VLAN basis 2-705 enabling spanning tree UplinkFast 2-703 setting an interface priority 2-702 setting drop threshold for 2-246 setting pathcost 2-678 setting the default pathcost calculation method 2-695 subinterface configuration mode, summary 1-6 SVI creating a Layer 3 interface on a VLAN 2-160 switching characteristics excluding from link-up calculation 2-717 modifying 2-717 returning to interfaces capture function 2-717 switchport 2-741 switchport interfaces displaying status of Layer 3 port 2-478 displaying status of native VLAN tagging 2-478 switch shim debugging 2-94 disabling debugging 2-94 switch to router connection enabling Cisco-recommended features 2-272

switch to switch connection
 enabling Cisco-recommended features 2-274
switch virtual interface
 See SVI
sw-vlan 2-97
system prompts 1-5

Т

Tab key command completion 1-1 tables characters with special meaning 1-7 mac access-list extended subcommands 2-258 multipliers 1-9 relationship between duplex and speed commands 2-708 show cable-diagnostics tdr command output fields **2-421** show cdp neighbors detail field descriptions 2-424 show cdp neighbors field descriptions 2-423 show ip interface field descriptions 2-513 show policy-map control-plane field descriptions 2-591 show vlan command output fields 2-658 show vtp command output fields 2-663 special characters 1-9 special characters used for anchoring 1-10 speed command options 2-286, 2-708 valid interface types 2-155 TAC displaying information useful to TAC 2-644 TCAM debugging spanning tree activities 2-91 TDR displaying cable diagnostic test results 2-420 test condition of copper cables 2-747 temperature readings displaying information 2-443

Ten-Gigabit Ethernet uplink blocking ports on redundant Supervisor Engine 6-E 2-149 timer information 2-447 traffic shaping enable on an interface 2-409 traps, enabling 2-669 trunk encapsulation setting format 2-741 trunk interfaces displaying trunk interfaces information 2-485 trust state setting 2-167 tunnel ports displaying information about Layer 2 protocol 2-554 TX queues allocating bandwidth 2-757 returning to default values 2-757 setting priority to high 2-757 specifying burst size 2-757 specifying traffic rate 2-757

U

UDLD displaying administrative and operational status 2-646 enabling by default on all fiber interfaces 2-759 enabling on an individual interface 2-761 preventing a fiber interface from being enabled 2-761 resetting all shutdown ports 2-763 setting the message timer 2-759 unicast counters 2-64 Unidirectional Link Detection See UDLD unknown multicast traffic, preventing 2-719 unknown unicast traffic, preventing 2-719 user EXEC mode, summary 1-5

username

setting password and privilege level 2-765

V

VACLs access-group mode 2-6 applying VLAN access maps 2-780 displaying VLAN access map information 2-652 specifying an action in a VLAN access map 2-13 specifying the match clause for a VLAN access-map sequence 2-281 using a VLAN filter 2-780 VLAN applying an ARP ACL 2-161 configuring 2-769 configuring service policies 2-774 converting to RSPAN VLAN 2-381 displaying CEF information 2-492 displaying CEF next-hop information 2-492 displaying information on switch interfaces 2-503, 2-507 displaying information on VLAN switch interfaces 2-510 displaying information sorted by group IP address 2-503, 2-507 displaying IP address and version information 2-503, 2-507 displaying Layer 2 VLAN information 2-648 displaying statistical information 2-582 displaying VLAN information 2-650 enabling dynamic ARP inspection 2-170 enabling Explicit Host Tracking 2-201 enabling guest per-port 2-117 enabling guest VLAN supplicant 2-110, 2-118 entering VLAN configuration mode 2-774, 2-776 native frames enabling tagging on all 802.1Q trunk ports 2-778 pruning the list for VTP 2-741 setting the list of allowed 2-741

VLAN Access Control Lists See VACLs VLAN access map See VACLs VLAN database resetting 2-383 VLAN debugging limiting output 2-72 VLAN link-up calculation excluding a switch port 2-717 including a switch port 2-717 VLAN manager debugging 2-97 disabling debugging 2-97 IOS file system error tests debugging 2-98 disabling debugging 2-98 VLAN Query Protocol See VQP VLAN query protocol (VQPC) debugging 2-104 **VLANs** clearing counters 2-60 clearing hardware logic 2-38 configuring internal allocation scheme 2-781 displaying internal VLAN allocation information 2-655 RSPAN VLANs 2-659 entering VLAN configuration mode 2-776 VMPS configuring servers 2-785 reconfirming dynamic VLAN assignments 2-104, 2-783 voice VLANs enabling 2-713 VoIP configuring auto-QoS 2-18

VOP per-server retry count 2-784 reconfirming dynamic VLAN assignments 2-104, 2-783 VTP configuring the administrative domain name 2-789 configuring the device in VTP client mode 2-788 configuring the device in VTP server mode 2-792 configuring the device in VTP transparent mode 2-793 configuring tunnel encapsulation rate 2-248 creating a VTP domain password 2-790 displaying domain information 2-662 displaying statistics information 2-662 enabling protocol tunneling for 2-243 enabling pruning in the VLAN database 2-791 enabling VTP version 2 mode 2-794 modifying the VTP configuration storage file name 2-787 set drop threshold for 2-246 VTP protocol code activating debug messages 2-101 deactivating debug messages 2-101

Catalyst 4500 Series Switch Cisco IOS Command Reference—Release 12.2(46)SG