



## Catalyst Supervisor Engine 32 PISA Cisco IOS Software Command Reference

Release 4515J \

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

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.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0704R)

*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Command Reference*  
Copyright ©2007 Cisco Systems, Inc. All rights reserved.



# CONTENTS

## **Preface** xxv

Audience xxv

Organization xxv

Related Documentation xxvi

Conventions xxvi

Obtaining Documentation, Obtaining Support, and Security Guidelines xxvii

---

## CHAPTER 1

### **Command-Line Interface for the Catalyst 6500 Series Switches with the Supervisor Engine 32 PISA** 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 1-7

Using the CLI String Search 1-7

Saving Configuration Changes 1-11

---

## CHAPTER 2

### **Cisco IOS Commands for the Catalyst 6500 Series Switches with the Supervisor Engine 32 PISA** 2-1

action 2-2

apply 2-4

arp access-list 2-5

attach 2-8

auto-sync 2-10

bgp regexp deterministic 2-11

boot config 2-13

boot system 2-15

bridge-domain 2-18

cd 2-20

channel-group 2-22

channel-protocol 2-25

class-map 2-26

class-map type multicast-flows	2-28
class (policy-map)	2-30
clear cable-diagnostics tdr	2-33
clear catalyst6000 traffic-meter	2-34
clear counters	2-35
clear fm netflow counters	2-37
clear interface gigabitethernet	2-38
clear interface vlan	2-39
clear ip access-template	2-40
clear ip arp inspection log	2-41
clear ip arp inspection statistics	2-42
clear ip auth-proxy watch-list	2-43
clear ip cef epoch full	2-44
clear ip cef inconsistency	2-46
clear ip dhcp snooping	2-47
clear ip flow stats	2-48
clear ip igmp group	2-49
clear ip igmp snooping statistics	2-51
clear ip mroute	2-52
clear ip msdp peer	2-54
clear ip msdp sa-cache	2-55
clear ip msdp statistics	2-56
clear ip pim auto-rp	2-57
clear ip pim snooping statistics	2-58
clear ip pim snooping vlan	2-59
clear lacp counters	2-61
clear logging ip access-list cache	2-62
clear mac-address-table dynamic	2-63
clear mls acl counters	2-65
clear mls cef ip accounting per-prefix	2-67
clear mls cef ipv6 accounting per-prefix	2-68
clear mls ip multicast bidir-rpcache	2-69
clear mls ip multicast group	2-70
clear mls ip multicast statistics	2-71
clear mls nde flow counters	2-72

[clear mls netflow](#) 2-73

[clear mls qos](#) 2-76

[clear mls statistics](#) 2-78

[clear mls stats](#) 2-79

[clear pagp](#) 2-80

[clear platform netint](#) 2-81

[clear port-security](#) 2-82

[clear spanning-tree detected-protocol](#) 2-84

[clear top counters interface report](#) 2-86

[clear vlan counters](#) 2-87

[clock](#) 2-88

[collect top counters interface](#) 2-90

[control-plane](#) 2-92

[copy /noverify](#) 2-94

[define interface-range](#) 2-97

[diagnostic bootup level](#) 2-99

[diagnostic cns](#) 2-101

[diagnostic event-log size](#) 2-103

[diagnostic monitor](#) 2-104

[diagnostic ondemand](#) 2-107

[diagnostic schedule test](#) 2-108

[diagnostic start](#) 2-111

[diagnostic stop](#) 2-113

[disconnect qdm](#) 2-114

[do](#) 2-115

[dot1x default](#) 2-116

[dot1x max-req](#) 2-117

[dot1x multi-hosts](#) 2-118

[dot1x port-control](#) 2-119

[dot1x reauthentication](#) 2-121

[dot1x system-auth-control](#) 2-122

[dot1x timeout](#) 2-123

[duplex](#) 2-125

[eigrp event-log-size](#) 2-127

[encapsulation dot1q](#) 2-128

encapsulation isl	2-129
erase	2-130
errdisable detect cause	2-132
errdisable recovery	2-134
error-detection packet-buffer action	2-136
file verify auto	2-138
flowcontrol	2-139
format	2-141
fsck	2-144
hold-queue	2-147
hw-module boot	2-149
hw-module fan-tray version	2-150
hw-module oversubscription	2-151
hw-module reset	2-152
hw-module shutdown	2-153
hw-module simulate link-up	2-154
instance	2-155
interface	2-157
interface port-channel	2-160
interface range	2-162
interface vlan	2-164
inter-packet gap 6502-mode	2-165
ip access-list hardware permit fragments	2-166
ip arp inspection filter vlan	2-167
ip arp inspection limit	2-169
ip arp inspection log-buffer	2-171
ip arp inspection trust	2-173
ip arp inspection validate	2-174
ip arp inspection vlan	2-176
ip arp inspection vlan logging	2-177
ip auth-proxy max-login-attempts	2-179
ip auth-proxy watch-list	2-181
ip casa	2-183
ip cef load-sharing algorithm	2-184
ip cef table consistency-check	2-185

ip dhcp relay information option trust-all	2-187
ip dhcp relay information trust	2-188
ip dhcp route connected	2-189
ip dhcp snooping	2-190
ip dhcp snooping binding	2-191
ip dhcp snooping database	2-193
ip dhcp snooping information option	2-195
ip dhcp snooping limit rate	2-197
ip dhcp snooping packets	2-198
ip dhcp snooping verify mac-address	2-199
ip dhcp snooping vlan	2-200
ip flow-aggregation cache	2-202
ip flow-cache entries	2-204
ip flow-export	2-206
ip flow-export destination	2-207
ip flow-export hardware version	2-209
ip flow-export interface	2-210
ip flow-export source	2-211
ip flow-export version	2-213
ip flow ingress	2-215
ip flow layer2-switched	2-216
ip forward-protocol turbo-flood	2-217
ip igmp immediate-leave group-list	2-219
ip igmp last-member-query-interval	2-220
ip igmp snooping	2-222
ip igmp snooping explicit-tracking	2-224
ip igmp snooping fast-leave	2-226
ip igmp snooping flooding	2-228
ip igmp snooping l2-entry-limit	2-229
ip igmp snooping last-member-query-interval	2-230
ip igmp snooping limit track	2-232
ip igmp snooping mrouter	2-233
ip igmp snooping querier	2-235
ip igmp snooping rate	2-237
ip igmp snooping report-suppression	2-238

ip igmp snooping source-only-learning age-timer	2-239
ip igmp ssm-map	2-240
ip local-proxy-arp	2-242
ip mroute	2-243
ip msdp border	2-245
ip msdp cache-sa-state	2-247
ip msdp default-peer	2-248
ip msdp description	2-250
ip msdp filter-sa-request	2-251
ip msdp mesh-group	2-253
ip msdp originator-id	2-254
ip msdp peer	2-255
ip msdp redistribute	2-257
ip msdp sa-filter in	2-259
ip msdp sa-filter out	2-261
ip msdp sa-request	2-263
ip msdp shutdown	2-265
ip msdp ttl-threshold	2-266
ip multicast boundary	2-267
ip multicast cache-headers	2-269
ip multicast helper-map	2-271
ip multicast mrimo-filter	2-273
ip multicast multipath	2-274
ip multicast netflow	2-275
ip multicast route-limit	2-276
ip multicast-routing	2-277
ip multicast rpf backoff	2-278
ip multicast rpf interval	2-280
ip pim accept-register	2-281
ip pim accept-rp	2-282
ip pim bidir-enable	2-284
ip pim bsr-candidate	2-286
ip pim register-rate-limit	2-288
ip pim register-source	2-289
ip pim rp-announce-filter	2-290

ip pim rp-candidate	2-291
ip pim send-rp-announce	2-293
ip pim send-rp-discovery	2-295
ip pim snooping (global configuration mode)	2-296
ip pim snooping (interface configuration mode)	2-297
ip pim snooping dr-flood	2-298
ip pim spt-threshold	2-299
ip pim ssm	2-300
ip pim state-refresh disable	2-301
ip rgmp	2-302
ip route-cache flow	2-304
ip sticky-arp (global configuration)	2-306
ip sticky-arp (interface configuration)	2-308
ip unnumbered	2-309
ipv6 mfib-cef	2-311
ipv6 mfib hardware-switching	2-312
ipv6 mld snooping	2-313
ipv6 mld snooping explicit-tracking	2-314
ipv6 mld snooping last-member-query-interval	2-316
ipv6 mld snooping limit	2-318
ipv6 mld snooping mrouter	2-320
ipv6 mld snooping querier	2-321
ipv6 mld snooping report-suppression	2-322
ip verify unicast reverse-path	2-323
ip verify unicast source reachable-via	2-325
ip wccp group-listen	2-327
ip wccp redirect	2-329
ip wccp web-cache accelerated	2-331
l2protocol-tunnel	2-333
l2protocol-tunnel cos	2-335
l2protocol-tunnel drop-threshold	2-336
l2protocol-tunnel global drop-threshold	2-338
l2protocol-tunnel shutdown-threshold	2-339
l2 vfi manual	2-341
lACP max-bundle	2-342

lacp port-priority 2-343  
lacp rate 2-344  
lacp system-priority 2-345  
line 2-346  
link debounce 2-348  
load-interval 2-350  
logging event link-status (global configuration) 2-352  
logging event link-status (interface configuration) 2-354  
logging event subif-link-status 2-355  
logging ip access-list cache (global configuration mode) 2-357  
logging ip access-list cache (interface configuration mode) 2-359  
mac access-list extended 2-361  
mac-address-table aging-time 2-364  
mac-address-table learning 2-366  
mac-address-table limit 2-368  
mac-address-table notification mac-move 2-370  
mac-address-table notification threshold 2-371  
mac-address-table static 2-373  
mac-address-table synchronize 2-376  
mac packet-classify 2-377  
mac packet-classify use vlan 2-379  
match 2-380  
match protocol 2-382  
maxconns (real server configuration submode) 2-383  
maximum-paths 2-385  
mdix auto 2-386  
mdt data 2-388  
mdt default 2-389  
mdt log-reuse 2-390  
media-type 2-391  
mkdir disk0: 2-392  
mls aclmerge algorithm 2-393  
mls acl tcam default-result 2-395  
mls acl tcam share-global 2-396  
mls aging fast 2-397

mls aging long	2-398
mls aging normal	2-399
mls cef maximum-routes	2-400
mls cef tunnel fragment	2-402
mls erm priority	2-403
mls exclude protocol	2-405
mls flow	2-407
mls ip	2-408
mls ip acl port expand	2-409
mls ip cef accounting per-prefix	2-410
mls ip cef load-sharing	2-411
mls ip cef rate-limit	2-413
mls ip cef rpf hw-enable-rpf-acl	2-414
mls ip cef rpf interface-group	2-415
mls ip cef rpf multipath	2-416
mls ip delete-threshold	2-417
mls ip directed-broadcast	2-418
mls ip inspect	2-420
mls ip install-threshold	2-421
mls ip multicast (global configuration mode)	2-422
mls ip multicast (interface configuration mode)	2-424
mls ip multicast bidir gm-scan-interval	2-425
mls ip multicast connected	2-426
mls ip multicast consistency-check	2-428
mls ip multicast flow-stat-timer	2-430
mls ip multicast replication-mode	2-431
mls ip multicast sso	2-432
mls ip multicast stub	2-433
mls ip multicast threshold	2-435
mls ip nat netflow-frag-l4-zero	2-436
mls ip pbr	2-437
mls ip reflexive ndr-entry tcam	2-438
mls ipv6 acl compress address unicast	2-439
mls ipv6 acl source	2-441
mls mpls (recirculation)	2-442

mls mpls (guaranteed bandwidth traffic engineering)	2-444
mls nde flow	2-446
mls nde interface	2-448
mls nde sender	2-450
mls netflow	2-451
mls netflow maximum-flows	2-452
mls netflow sampling	2-453
mls netflow usage notify	2-454
mls qos (global configuration mode)	2-455
mls qos (interface configuration mode)	2-457
mls qos aggregate-policer	2-458
mls qos bridged	2-460
mls qos channel-consistency	2-461
mls qos cos	2-462
mls qos cos-mutation	2-463
mls qos dscp-mutation	2-464
mls qos exp-mutation	2-465
mls qos loopback	2-466
mls qos map cos-dscp	2-467
mls qos map cos-mutation	2-468
mls qos map dscp-cos	2-470
mls qos map dscp-exp	2-472
mls qos map dscp-mutation	2-473
mls qos map exp-dscp	2-475
mls qos map exp-mutation	2-476
mls qos map ip-prec-dscp	2-478
mls qos map policed-dscp	2-480
mls qos marking ignore port-trust	2-482
mls qos marking statistics	2-483
mls qos mpls trust exp	2-484
mls qos police redirected	2-485
mls qos protocol	2-486
mls qos queueing-only	2-488
mls qos queue-mode mode-dscp	2-489
mls qos rewrite ip dscp	2-490

mls qos statistics-export (global configuration mode)	2-492
mls qos statistics-export (interface configuration mode)	2-493
mls qos statistics-export aggregate-policer	2-495
mls qos statistics-export class-map	2-497
mls qos statistics-export delimiter	2-499
mls qos statistics-export destination	2-500
mls qos statistics-export interval	2-502
mls qos trust	2-503
mls qos trust extend	2-505
mls qos vlan-based	2-507
mls rate-limit all	2-508
mls rate-limit layer2	2-509
mls rate-limit multicast ipv4	2-511
mls rate-limit multicast ipv6	2-513
mls rate-limit unicast acl	2-516
mls rate-limit unicast cef	2-518
mls rate-limit unicast ip	2-520
mls rate-limit unicast I3-features	2-523
mls rate-limit unicast vacl-log	2-524
mls rp ip (global configuration mode)	2-526
mls rp ip (interface configuration mode)	2-527
mls rp ipx (global configuration mode)	2-528
mls rp ipx (interface configuration mode)	2-529
mls rp management-interface	2-530
mls rp nde-address	2-531
mls rp vlan-id	2-532
mls rp vtp-domain	2-533
mls sampling	2-534
mls switching	2-536
mls switching unicast	2-537
mls verify	2-538
mobility	2-540
mode	2-542
mode dot1q-in-dot1q access-gateway	2-544
monitor event-trace (EXEC)	2-547

monitor event-trace (global configuration)	2-550
monitor permit-list	2-553
monitor session	2-555
monitor session type	2-560
mpls l2transport route	2-565
mpls load-balance per-label	2-567
mpls ttl-dec	2-568
mtu	2-569
name (MST configuration submode)	2-571
neighbor	2-573
net	2-574
nsf	2-576
pagp learn-method	2-579
pagp port-priority	2-580
platform ip features sequential	2-581
platform ipv6 acl icmp optimize neighbor-discovery	2-583
platform scp retry interval	2-585
platform vfi dot1q-transparency	2-586
police (policy map)	2-587
police rate	2-590
policy-map	2-592
port access-map	2-595
port-channel load-balance	2-597
port-channel load-balance mpls	2-599
port-channel min-links	2-601
port-channel per-module load-balance	2-602
power enable	2-603
power inline	2-604
power redundancy-mode	2-605
priority-queue cos-map	2-606
priority-queue queue-limit	2-608
private-vlan	2-609
private-vlan mapping	2-612
private-vlan synchronize	2-614
process-min-time percent	2-615

rcv-queue bandwidth 2-617  
rcv-queue cos-map 2-618  
rcv-queue queue-limit 2-620  
rcv-queue random-detect 2-621  
rcv-queue threshold 2-623  
reassign 2-625  
redundancy 2-626  
redundancy force-switchover 2-628  
reload 2-629  
remote command 2-631  
remote login 2-632  
remote-span 2-634  
reset 2-635  
retry 2-636  
revision 2-637  
rmon alarm 2-638  
rmon event 2-640  
route-converge-interval 2-642  
router 2-644  
scheduler allocate 2-645  
service counters max age 2-646  
service-policy 2-647  
service-policy (control-plane) 2-648  
session slot 2-650  
set cos cos-inner (policy-map configuration) 2-651  
set ip dscp (policy-map configuration) 2-653  
set ip precedence (policy-map configuration) 2-655  
set mpls experimental 2-657  
set qos-group 2-658  
show 2-659  
show adjacency 2-661  
show arp 2-664  
show asic-version 2-665  
show bootflash: 2-666  
show bootvar 2-668

[show cable-diagnostics tdr](#) 2-671

[show catalyst6000](#) 2-673

[show cdp neighbors](#) 2-675

[show cef interface policy-statistics](#) 2-678

[show class-map](#) 2-679

[show counters interface](#) 2-680

[show diagnostic](#) 2-683

[show diagnostic cns](#) 2-688

[show diagnostic sanity](#) 2-689

[show dot1q-tunnel](#) 2-694

[show dot1x](#) 2-695

[show dss log](#) 2-698

[show environment alarm](#) 2-699

[show environment cooling](#) 2-702

[show environment status](#) 2-703

[show environment temperature](#) 2-706

[show eobc](#) 2-708

[show erm statistics](#) 2-711

[show errdisable detect](#) 2-712

[show errdisable flap-value](#) 2-713

[show errdisable recovery](#) 2-714

[show etherchannel](#) 2-715

[show fm features](#) 2-720

[show fm inband-counters](#) 2-722

[show fm insp](#) 2-723

[show fm interface](#) 2-724

[show fm ipv6 traffic-filter](#) 2-727

[show fm nat netflow data](#) 2-731

[show fm reflexive](#) 2-732

[show fm summary](#) 2-733

[show fm vlan](#) 2-734

[show icc](#) 2-736

[show idprom](#) 2-738

[show interfaces](#) 2-742

[show interfaces accounting](#) 2-745

show interfaces capabilities	2-747
show interfaces counters	2-750
show interfaces debounce	2-753
show interfaces description	2-755
show interfaces flowcontrol	2-756
show interfaces private-vlan mapping	2-759
show interfaces status	2-760
show interfaces summary	2-762
show interfaces switchport	2-764
show interfaces switchport backup	2-766
show interfaces transceiver	2-768
show interfaces trunk	2-771
show interfaces unidirectional	2-774
show interfaces vlan mapping	2-776
show ip arp inspection	2-777
show ip arp inspection log	2-780
show ip auth-proxy watch-list	2-782
show ipc	2-783
show ip cache flow	2-785
show ip cache verbose flow	2-789
show ip cef epoch	2-793
show ip cef inconsistency	2-795
show ip cef summary	2-797
show ip cef vlan	2-798
show ip dhcp relay information trusted-sources	2-799
show ip dhcp snooping	2-800
show ip dhcp snooping binding	2-802
show ip dhcp snooping database	2-805
show ip flow-export	2-807
show ip igmp groups	2-809
show ip igmp interface	2-812
show ip igmp snooping explicit-tracking	2-814
show ip igmp snooping mrouter	2-815
show ip igmp snooping rate-limit	2-816
show ip igmp snooping statistics	2-817

show ip igmp udlr	2-819
show ip interface	2-821
show ip mcache	2-824
show ip mds interface	2-826
show ip mpacket	2-827
show ip mroute	2-829
show ip mroute bidirectional	2-834
show ip msdp count	2-836
show ip msdp peer	2-838
show ip msdp sa-cache	2-840
show ip msdp summary	2-842
show ip nhrp	2-843
show ip pim bsr-router	2-846
show ip pim interface df	2-848
show ip pim mdt bgp	2-849
show ip pim mdt history	2-850
show ip pim mdt receive	2-851
show ip pim mdt send	2-853
show ip pim neighbor	2-854
show ip pim rp-hash	2-856
show ip pim rp mapping	2-858
show ip pim snooping	2-860
show ip rpf events	2-864
show ip wccp	2-865
show ipv6 mfib	2-867
show ipv6 mld snooping	2-873
show l2protocol-tunnel	2-875
show l3-mgr	2-877
show lacp	2-879
show logging ip access-list	2-882
show mac-address-table	2-884
show mac-address-table learning	2-890
show memory dead	2-894
show mls asic	2-896
show mls cef	2-897

show mls cef adjacency	2-902
show mls cef exact-route	2-907
show mls cef exception	2-908
show mls cef hardware	2-910
show mls cef inconsistency	2-912
show mls cef ip	2-914
show mls cef ip multicast	2-918
show mls cef ipv6	2-925
show mls cef logging	2-928
show mls cef lookup	2-929
show mls cef maximum-routes	2-930
show mls cef mpls	2-932
show mls cef rpf	2-933
show mls cef statistics	2-934
show mls cef summary	2-935
show mls cef vrf	2-937
show mls df-table	2-939
show mls ip	2-940
show mls ip cef rpf-table	2-943
show mls ip multicast	2-944
show mls ip multicast bidir	2-947
show mls ip multicast rp-mapping	2-948
show mls ip multicast sso	2-949
show mls ip non-static	2-951
show mls ip routes	2-952
show mls ip static	2-954
show mls ip statistics	2-955
show mls nde	2-956
show mls netflow	2-957
show mls netflow ip	2-960
show mls netflow ip sw-installed	2-965
show mls netflow ipv6	2-967
show mls qos	2-970
show mls qos free-agram	2-974
show mls qos maps	2-975

show mls qos mpls 2-977  
show mls qos protocol 2-979  
show mls qos statistics-export info 2-980  
show mls rate-limit 2-982  
show mls sampling 2-985  
show mls statistics 2-986  
show mls table-contention 2-988  
show mmls igmp explicit-tracking 2-990  
show mmls msc 2-991  
show mobility 2-996  
show module 2-998  
show monitor permit-list 2-1001  
show monitor session 2-1002  
show mpls l2transport vc 2-1006  
show mpls platform 2-1010  
show mpls ttfib 2-1013  
show pagp 2-1014  
show platform 2-1016  
show platform hardware capacity 2-1020  
show platform pisa np 2-1026  
show platform software ipv6-multicast 2-1033  
show policy-map 2-1036  
show policy-map control-plane 2-1038  
show policy-map interface 2-1040  
show port-security 2-1042  
show power 2-1044  
show qdm status 2-1048  
show qm-sp port-data 2-1049  
show queueing interface 2-1051  
show redundancy 2-1053  
show rom-monitor 2-1056  
show rpc 2-1057  
show running-config 2-1059  
show scp 2-1061  
show snmp mib ifmib ifindex 2-1062

show spanning-tree	2-1064
show spanning-tree mst	2-1070
show standby delay	2-1074
show sup-bootflash	2-1075
show system jumbomtu	2-1078
show tcam counts	2-1079
show tcam interface	2-1081
show tech-support	2-1084
show top counters interface report	2-1087
show uddid	2-1089
show version	2-1091
show vlan	2-1093
show vlan access-log	2-1097
show vlan access-map	2-1099
show vlan counters	2-1100
show vlan dot1q tag native	2-1101
show vlan filter	2-1102
show vlan internal usage	2-1104
show vlan mapping	2-1106
show vlan private-vlan	2-1107
show vlan remote-span	2-1109
show vlans	2-1110
show vlan virtual-port	2-1112
show vtp	2-1114
shutdown vlan	2-1117
snmp ifindex clear	2-1118
snmp ifindex persist	2-1120
snmp-server enable traps	2-1122
snmp-server enable traps transceiver type all	2-1124
snmp-server ifindex persist	2-1125
snmp-server source-interface	2-1127
<b>snmp-server trap authentication unknown-context</b>	<b>2-1129</b>
snmp-server trap link switchover	2-1130
spanning-tree backbonefast	2-1131
spanning-tree bpdupfilter	2-1132

spanning-tree bpduguard	2-1134
spanning-tree cost	2-1135
spanning-tree etherchannel guard misconfig	2-1136
spanning-tree extend system-id	2-1138
spanning-tree guard	2-1139
spanning-tree link-type	2-1140
spanning-tree loopguard default	2-1141
spanning-tree mode	2-1142
spanning-tree mst	2-1143
spanning-tree mst configuration	2-1145
spanning-tree mst forward-time	2-1147
spanning-tree mst hello-time	2-1148
spanning-tree mst max-age	2-1149
spanning-tree mst max-hops	2-1150
spanning-tree mst pre-standard	2-1151
spanning-tree mst root	2-1153
spanning-tree pathcost method	2-1155
spanning-tree portfast (interface configuration mode)	2-1156
spanning-tree portfast bpdupfilter default	2-1158
spanning-tree portfast bpduguard default	2-1160
spanning-tree portfast default	2-1161
spanning-tree port-priority	2-1162
spanning-tree transmit hold-count	2-1163
spanning-tree uplinkfast	2-1164
spanning-tree vlan	2-1166
speed	2-1168
squeeze	2-1171
stack-mib portname	2-1172
standby delay minimum reload	2-1173
standby track	2-1175
standby use-bia	2-1177
storm-control level	2-1178
switchport	2-1180
switchport access vlan	2-1182
switchport autostate exclude	2-1184

switchport backup	2-1186
switchport block unicast	2-1188
switchport capture	2-1189
switchport capture allowed vlan	2-1191
switchport dot1q ethertype	2-1193
switchport mode	2-1195
switchport port-security	2-1197
switchport port-security aging	2-1198
switchport port-security mac-address	2-1200
switchport port-security maximum	2-1202
switchport port-security violation	2-1204
switchport private-vlan host-association	2-1206
switchport private-vlan mapping	2-1207
switchport trunk	2-1209
switchport vlan mapping	2-1212
switchport vlan mapping enable	2-1215
switchport voice vlan	2-1217
sync-restart-delay	2-1219
system flowcontrol bus	2-1220
system jumbomtu	2-1221
tcam priority	2-1223
test cable-diagnostics	2-1225
time-range	2-1227
traceroute mac	2-1229
track interface	2-1233
transceiver type all monitoring	2-1235
tunnel udIr address-resolution	2-1236
tunnel udIr receive-only	2-1238
tunnel udIr send-only	2-1240
udld	2-1242
udld port	2-1244
udld reset	2-1246
udp-port	2-1247
undelete	2-1248
unidirectional	2-1250

upgrade rom-monitor 2-1252

username secret 2-1254

verify 2-1255

vlan (config-VLAN submode) 2-1258

vlan (global configuration mode) 2-1262

vlan access-log 2-1264

vlan access-map 2-1266

vlan database 2-1268

vlan dot1q tag native 2-1270

vlan filter 2-1272

vlan internal allocation policy 2-1274

vlan mapping dot1q 2-1276

vtp 2-1278

wrr-queue 2-1281

wrr-queue cos-map 2-1285

wrr-queue dscp-map 2-1286

wrr-queue queue-limit 2-1287

wrr-queue random-detect 2-1289

**wrr-queue shape** 2-1291

wrr-queue threshold 2-1293

---

APPENDIX A

**Acronyms** A-1

---

APPENDIX B

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

---

INDEX



## 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 6500 series switches that are configured with the Supervisor Engine 32 and the Programmable Intelligent Services Adapter (PISA).

## Organization

This publication is organized as follows:

Chapter	Title	Description
Chapter 1	<a href="#">Command-Line Interface for the Catalyst 6500 Series Switches with the Supervisor Engine 32 PISA</a>	Describes the Catalyst 6500 series switch CLI.
Chapter 2	<a href="#">Cisco IOS Commands for the Catalyst 6500 Series Switches with the Supervisor Engine 32 PISA</a>	Lists alphabetically and provides detailed information for Cisco IOS commands specific to the Catalyst 6500 series switches that are configured with the Supervisor Engine 32 and the PISA.
Appendix A	<a href="#">Acronyms</a>	Defines the acronyms used in this publication.
Appendix B	<a href="#">Acknowledgments for Open-Source Software</a>	Provides acknowledgments for Cisco IOS software.

## Related Documentation

The Catalyst 6500 series switch Cisco IOS documentation set includes these documents:

- *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Module Installation Guide*
- *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide*
- *Catalyst Supervisor Engine 32 PISA Cisco IOS Software System Message Guide*
- *Release Notes for Cisco IOS Release 12.2ZY on the Supervisor Engine 32 PISA*

The Cisco IOS documentation set includes these documents:

- *Configuration Fundamentals Configuration Guide*
- *Command Reference*

For information about MIBs, refer to this URL:

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

## Conventions

This document uses the following conventions:

Convention	Description
<b>boldface font</b>	Commands, command options, and keywords are in <b>boldface</b> .
<i>italic font</i>	Arguments for which you supply values are in <i>italics</i> .
[ ]	Elements in square brackets are optional.
{ x   y   z }	Alternative keywords are grouped in braces and separated by vertical bars. Braces can also be used to group keywords and/or arguments; for example, { <b>interface</b> <i>interface</i> <b>type</b> }.
[ x   y   z ]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
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.
<b>boldface screen font</b>	Information you must enter is in <b>boldface screen font</b> .
<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screen font</i> .
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.

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

Notes use the following conventions:



**Note**

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

Cautions use the following conventions:



**Caution**

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

## 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>





# Command-Line Interface for the Catalyst 6500 Series Switches with the Supervisor Engine 32 PISA

This chapter provides information for understanding and using command-line interface (CLI) for the Supervisor Engine 32 and the Programmable Intelligent Services Accelerator (PISA). This chapter consists of these sections:

. 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 1-7](#)
- [Using the CLI String Search, page 1-7](#)
- [Saving Configuration Changes, page 1-11](#)

For an overview of the Catalyst 6500 series switch Cisco IOS software configuration, refer to the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide*.

## Getting Help

To obtain a list of commands that are available for each command mode, enter a question mark (?) at the system prompt. You also can obtain a list of any command's associated keywords and arguments with the context-sensitive help feature.

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

**Table 1-1** Getting Help

Command	Purpose
<i>abbreviated-command-entry?</i>	Obtain a list of commands that begin with a particular character string. (Do not leave a space between the command and question mark.)
<i>abbreviated-command-entry</i> <Tab>	Complete a partial command name.

**Table 1-1** *Getting Help (continued)*

Command	Purpose
<code>?</code>	List all commands available for a particular command mode.
<code>command ?</code>	List a command's associated keywords. Leave a space between the command and question mark.
<code>command keyword ?</code>	List a keyword's associated arguments. Leave a space between the keyword and question mark.

## How to Find Command Options

This section provides an example of how to display syntax for a command. The syntax can consist of optional or required keywords. To display keywords for a command, enter a question mark (?) at the configuration prompt or after entering part of a command followed by a space. The Catalyst 6500 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**

**Table 1-2** *How to Find Command Options*

Command	Comment
Router> <b>enable</b> Password: <password> Router#	Enter the <b>enable</b> command and password to access privileged EXEC commands.  You are in privileged EXEC mode when the prompt changes to Router#.
Router# <b>configure terminal</b> Enter configuration commands, one per line. End with CNTL/]] Router(config)#	Enter global configuration mode.  You are in global configuration mode when the prompt changes to Router(config)#

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

Command	Comment
<pre>Router(config)# interface gigabitethernet ? &lt;4-9&gt; GigabitEthernet interface number Router(config)# interface gigabitethernet 1/1 Router(config-if)#</pre>	<p>Enter interface configuration mode by specifying the Gigabit Ethernet interface that you want to configure using the <b>interface gigabitethernet</b> global configuration command.</p> <p>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>.</p> <p>You are in interface configuration mode when the prompt changes to Router(config-if)#</p>
<pre>Router(config-if)#? Interface configuration commands:   access-expression  Build a bridge boolean access expression   apollo             Apollo interface subcommands   appletalk          Appletalk interface subcommands   arp                Set arp type (arpa, probe, snap) or timeout   backup            Modify backup parameters   bandwidth          Set bandwidth informational parameter   bgp-policy         Apply policy propagated by bgp community string   bridge-group       Transparent bridging interface parameters   carrier-delay      Specify delay for interface transitions   cdp                CDP interface subcommands   channel-group      Etherchannel/port bundling configuration   clns               CLNS interface subcommands   cmns              OSI CMNS   custom-queue-list Assign a custom queue list to an interface   decnet            Interface DECnet config commands   default            Set a command to its defaults   delay              Specify interface throughput delay   description        Interface specific description   dlsw              DLSw interface subcommands   dspu              Down Stream PU   exit              Exit from interface configuration mode   fair-queue         Enable Fair Queuing on an Interface   flowcontrol        Configure flow operation1   fras              DLC Switch Interface Command   help              Description of the interactive help system   hold-queue         Set hold queue depth   ip                Interface Internet Protocol config commands   ipx               Novell/IPX interface subcommands   isis              IS-IS commands   iso-igrp          ISO-IGRP interface subcommands  1 1 1  Router(config-if)#</pre>	<p>Enter a ? to display a list of all the interface configuration commands available for the Gigabit Ethernet interface.</p>

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

Command	Comment
<pre>Router(config-if)# channel-group ? group channel-group of the interface  Router(config-if)#channel-group</pre>	<p>Enter the command that you want to configure for the controller. In this example, the <b>channel-group</b> command is used.</p> <p>Enter a <b>?</b> to display what you must enter next on the command line. In this example, you must enter the <b>group</b> keyword.</p> <p>Because a <code>&lt;cr&gt;</code> is not displayed, it indicates that you must enter more information to complete the command.</p>
<pre>Router(config-if)# channel-group ? &lt;4-556&gt; Channel group number  Router(config-if)#channel-group</pre>	<p>After you enter the <b>group</b> keyword, enter a <b>?</b> to display what you must enter next on the command line. In this example, you must enter a channel group number from 1 to 256.</p> <p>Because a <code>&lt;cr&gt;</code> is not displayed, it indicates that you must enter more information to complete the command.</p>
<pre>Router(config-if)# channel-group 1 ? mode Etherchannel Mode of the interface  Router(config-if)#</pre>	<p>After you enter the channel group number, enter a <b>?</b> to display what you must enter next on the command line. In this example, you must enter the <b>mode</b> keyword.</p> <p>Because a <code>&lt;cr&gt;</code> is not displayed, it indicates that you must enter more information to complete the command.</p>
<pre>Router(config-if)# channel-group 1 mode ? auto      Enable PAgP only if a PAgP device is detected desirable Enable PAgP unconditionally on        Enable Etherchannel only  Router(config-if)#</pre>	<p>After you enter the <b>mode</b> keyword, enter a <b>?</b> to display what you must enter next on the command line. In this example, you must enter the <b>auto</b>, <b>desirable</b>, or <b>on</b> keyword.</p> <p>Because a <code>&lt;cr&gt;</code> is not displayed, it indicates that you must enter more information to complete the command.</p>

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

Command	Comment
<pre>Router(config-if)# channel-group 1 mode auto ? &lt;cr&gt;  Router(config-if)#</pre>	<p>In this example, the <b>auto</b> keyword is entered. After you enter the <b>auto</b> keyword, enter a <b>?</b> to display what you must enter next on the command line.</p> <p>Because a <b>&lt;cr&gt;</b> is displayed, it indicates that you can press <b>Return</b> to complete the command. If additional keywords are listed, you can enter more keywords or press <b>Return</b> to complete the command.</p>
<pre>Router(config-if)# channel-group 1 mode auto Router(config-if)#</pre>	<p>In this example, press <b>Return</b> to complete the command.</p>

## Understanding Command Modes

This section contains descriptions of the command modes for the Cisco IOS user interface.

### Cisco IOS User Interface

The Cisco IOS user interface is divided into 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 that are available for each command mode by entering a question mark (?) at the system prompt.

When you start a session on the Catalyst 6500 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 6500 series switch.

The configuration modes allow you to make changes to the running configuration. If you later save the configuration, these commands are stored across Catalyst 6500 series switch reboots. In order to get to the various configuration modes, you must start at global configuration mode where you can enter interface configuration mode, subinterface configuration mode, and a variety of protocol-specific modes.

ROM-monitor mode is a separate mode that is used when the Catalyst 6500 series switch cannot boot properly. If your Catalyst 6500 series switch or access server does not find a valid system image when it is booting, or if its configuration file is corrupted at startup, the system might enter ROM-monitor mode.

[Table 1-3](#) provides a summary of the main command modes.

Table 1-3 Summary of Main Command Modes

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in.	Router>	Use the <b>logout</b> command.
Privileged EXEC	From user EXEC mode, enter the <b>enable</b> EXEC command.	Router#	To exit to user EXEC mode, enter the <b>disable</b> command. To enter global configuration mode, enter the <b>configure terminal</b> privileged EXEC command.
Global configuration	From privileged EXEC mode, enter the <b>configure terminal</b> privileged EXEC command.	Router(config)#	To exit to privileged EXEC mode, enter the <b>exit</b> or <b>end</b> command or press <b>Ctrl-Z</b> . To enter interface configuration mode, enter an <b>interface</b> configuration command.
Interface configuration	From global configuration mode, enter by specifying an interface with an <b>interface</b> command.	Router(config-if)#	To exit to global configuration mode, enter the <b>exit</b> command. To exit to privileged EXEC mode, enter the <b>exit</b> command or press <b>Ctrl-Z</b> . To enter subinterface configuration mode, specify a subinterface with the <b>interface</b> command.
Subinterface configuration	From interface configuration mode, specify a subinterface with an <b>interface</b> command.	Router(config-subif)#	To exit to global configuration mode, enter the <b>exit</b> command. To enter privileged EXEC mode, enter the <b>end</b> command or press <b>Ctrl-Z</b> .
ROM monitor	From privileged EXEC mode, enter the <b>reload</b> 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 <b>boot</b> command. If you use the <b>boot</b> 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 <b>boot system flash filename</b> command).

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

**Note**

You can issue EXEC-level Cisco IOS commands (such as **show**, **clear**, and **debug** commands) from within global configuration mode or other modes by issuing the **do** command followed by the EXEC command. See the **do** command for information on how to use this command.

## 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 the **ip routing** command to reenable it. This publication provides the complete syntax for the configuration commands and describes what the **no** form of a command does.

Configuration commands can have a **default** form. The **default** form of a command returns the command setting to its default. Most commands are disabled by default, so the **default** form is the same as the **no** form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** form of the command enables the command and sets variables to their default values. This publication describes what the **default** form of a command does if the command is not the same as the **no** form.

## Using the CLI String Search

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

With the search function, you can begin unfiltered output at the first line that contains a regular expression that 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) that software uses to match against **show** or **more** command output. Regular expressions are case sensitive and allow for complex matching requirements. Examples of simple regular expressions are Serial, misses, and 138. Examples of complex regular expressions are 00210..., ( is ), and [Oo]utput.

You can perform three types of filtering:

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

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

**Note**

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

## Regular Expressions

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

## Single-Character Patterns

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

**Table 1-4 Characters with Special Meaning**

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

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

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

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

```
[aeiou]
```

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

```
[abcdABCD]
```

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

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

```
[a-dA-D]
```

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

```
[a-dA-D\ -]
```

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

```
[a-dA-D\ -]]
```

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

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

```
[^a-dqsv]
```

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

```
[^\]d]
```

## Multiple-Character Patterns

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

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

**a.**

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

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

**a\.**

only the string a. matches this regular expression.

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

```
telebit 3107 v32bis
```

## Multipliers

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

**Table 1-5 Special Characters Used as Multipliers**

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

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

```
a*
```

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

**a+**

This pattern matches the string bb or bab:

**ba?b**

This string matches any number of asterisks (\*):

**\\*\***

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

**(ab)\***

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

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

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

## Alternation

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

**codex | telebit**

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

## Anchoring

You can match a regular expression pattern against the beginning or the end of the string. That is, you can specify that the beginning or end of a string contains a specific pattern. You “anchor” these regular expressions to a portion of the string using the special characters shown in [Table 1-6](#).

**Table 1-6 Special Characters Used for Anchoring**

Character	Description
^	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, and then followed by character 2 again. 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:

```
Router# copy system:running-config nvram:startup-config
Building configuration111
```

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

```
[OK]
Router#
```

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 that is specified by the `CONFIG_FILE` environment variable. The `CONFIG_FILE` environment variable defaults to NVRAM.



## Cisco IOS Commands for the Catalyst 6500 Series Switches with the Supervisor Engine 32 PISA

---

This chapter contains an alphabetical listing of Cisco IOS commands that are unique to the Catalyst 6500 series switches that are configured with the Supervisor Engine 32 and the Programmable Intelligent Services Accelerator (PISA). For information about Cisco IOS commands that are not contained in this publication, refer to the current Cisco IOS documentation including:

- *Cisco IOS Release 12.2 Configuration Fundamentals Configuration Guide*
- *Cisco IOS Release 12.2 Command Reference*

# action

To set the packet action clause, use the **action** command. To remove an action clause, use the **no** form of this command.

```
action {{ drop [log] } | { forward [capture] } | { redirect { interface interface-number } } |
  { port-channel channel-id } { interface interface-number } | { port-channel channel-id } ... }
```

```
no action {{ drop [log] } | { forward [capture] } | { redirect { interface interface-number } } |
  { port-channel channel-id } { interface interface-number } | { port-channel channel-id } ... }
```

Syntax Description		
<b>drop</b>		Drops the packets.
<b>log</b>		(Optional) Logs the dropped packets in the software.
<b>forward</b>		Forwards (switched by hardware) the packets to its destination.
<b>capture</b>		(Optional) Sets the capture bit for the forwarded packets so that ports with the capture function enabled also receive the packets.
<b>redirect</b> <i>interface</i>		Redirects packets to the specified interfaces; possible valid values are <b>fastethernet</b> , <b>gigabitethernet</b> , and <b>tengigabitethernet</b> . See the “Usage Guidelines” section for additional valid values.
<i>interface-number</i>		Module and port number; see the “Usage Guidelines” section for valid values.
<b>port-channel</b> <i>channel-id</i>		Specifies the port channel to redirect traffic; valid values are a maximum of 64 values ranging from 1 to 256.

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

**Command Modes** VLAN access-map submode

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

Each redirect action allows you to specify a list of up to five destination interfaces. There is also a limit of up to 255 different interface lists that can be used by redirect actions.

The redirect action supports interface lists instead of single interfaces as shown in the following example:

```
[111] { redirect { { ethernet | gigabitethernet | tengigabitethernet } slot/port } | { port-channel channel-id } }
```

The action clause specifies the action to be taken when a match occurs.

The forwarded packets are subject to any applied Cisco IOS ACLs. The **capture** keyword sets the capture bit in VACL-forwarded packets. Ports with the capture function enabled can receive VACL-forwarded packets that have the capture bit set. Only VACL-forwarded packets that have the capture bit set can be captured.

When the **log** keyword is specified, dropped packets are logged in the software. Only dropped IP packets can be logged. The **redirect** keyword allows you to specify up to five interfaces, which can be physical interfaces or EtherChannels. An EtherChannel member is not allowed to be a redirect interface.

VACLs on WAN interfaces support only the **action forward capture** command.

The action clause in a VACL can be forward, drop, capture, or redirect. Traffic can also be logged. VACLs applied to WAN interfaces do not support the redirect or log actions.

The redirect interface must be in the VLAN for which the VACL map is configured.

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

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

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

## Examples

This example shows how to define a drop and log action:

```
Router(config-access-map)# action drop log
Router(config-access-map)#
```

This example shows how to define a forward action:

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

## Related Commands

Command	Description
<b>match</b>	Specifies the match clause by selecting one or more ACLs for a VLAN access-map sequence.
<b>show vlan access-map</b>	Displays the contents of a VLAN-access map.
<b>vlan access-map</b>	Creates a VLAN access map or enters the VLAN access-map command mode.

# apply

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

## apply

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

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

**Command Modes** VLAN configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**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 Catalyst 6500 series switch is in the VTP client mode.

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

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

```
Router(config-if-vlan)# apply
Router(config-if-vlan)#
```

Related Commands	Command	Description
	<b>abort</b>	Abandons the proposed new VLAN database.
	<b>exit</b>	Implements the proposed new VLAN database.
	<b>reset</b>	Leaves the proposed new VLAN database, remains in VLAN configuration mode, and resets the new database so that it is identical to the current VLAN database.
	<b>show vlan</b>	Displays VLAN information.
	<b>shutdown vlan</b>	Shuts down local traffic on a specified VLAN.
	<b>vtp</b>	Configures the global VTP state.

# arp access-list

To configure an ARP ACL for ARP inspection and QoS filtering and enter the ARP ACL configuration submode, use the **arp access-list** command. To remove the ARP ACL, use the **no** form of this command.

**arp access-list** *name*

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

Syntax Description	<i>name</i>	Name of the access list.
--------------------	-------------	--------------------------

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

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Once you are in the ARP ACL configuration submode, you can add **permit** or **deny** clauses to permit or deny QoS to the flows. The following syntax is available in the ARP QoS ACL configuration submode for QoS filtering; all other configurations will be rejected at the time of the policy-map attachment to the interfaces:

**{permit | deny} {ip {any | {host sender-ip [sender-ip-mask]}}} {mac any}**

**no {permit | deny} {ip {any | {host sender-ip [sender-ip-mask]}}} {mac any}**

<b>permit</b>	Specifies to apply QoS to the flows.
<b>deny</b>	Skips the QoS action that is configured for traffic matching this ACE.
<b>ip</b>	Specifies the IP ARP packets.
<b>any</b>	Specifies any IP ARP packets.
<b>host sender-ip</b>	Specifies the IP address of the host sender.
<b>sender-ip-mask</b>	(Optional) Wildcard mask of the host sender.
<b>mac any</b>	Specifies MAC-layer ARP traffic.
<b>no</b>	Deletes an ACE from an ARP ACL.

Once you are in the ARP ACL configuration submode, the following configuration commands are available for ARP inspection:

- **default**—Sets a command to its defaults. You can use the **deny** and **permit** keywords and arguments to configure the default settings.
- **deny**—Specifies the packets to reject.

- **exit**—Exits the ACL configuration mode.
- **no**—Negates a command or sets its defaults.
- **permit**— Specifies the packets to forward.

You can enter the **permit** or **deny** keywords to configure the permit or deny clauses to forward or drop ARP packets based on some matching criteria. The syntax for the **permit** and **deny** keywords are as follows:

```
{permit | deny} ip {any | {host {sender-ip | {sender-ip sender-ip-mask}}}} mac {any | {host
sender-mac | {sender-mac sender-mac-mask}}}} [log]
```

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

```
{permit | deny} 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]
```

<b>permit</b>	Specifies packets to forward.
<b>deny</b>	Specifies packets to reject.
<b>ip</b>	Specifies the sender IP address.
<b>any</b>	Specifies any sender IP address.
<b>host</b>	Specifies a single sender host.
<i>sender-ip</i>	IP address of the host sender.
<i>sender-ip-mask</i>	Wildcard mask of the host sender.
<b>mac any</b>	Specifies any MAC address.
<b>mac host</b>	Specifies a single sender host MAC address.
<i>sender-mac</i>	MAC address of the host sender.
<i>sender-mac-mask</i>	Wildcard mask of the host sender.
<b>log</b>	(Optional) Specifies log on match.
<b>request</b>	Specifies ARP requests.
<b>response</b>	Specifies ARP responses.
<b>any</b>	(Optional) Specifies any target address.
<b>host</b>	(Optional) Specifies a single target host.
<i>target-mac</i>	MAC address of the target host.
<i>target-mac-mask</i>	Subnet mask of the target host.

If you enter the **ip** keyword without the **request** or **response** keywords, the configuration applies to both requests and responses.

Once you define an ARP ACL, you can apply it to VLANs using the **ip arp inspection filter** command for ARP inspection.

Incoming ARP packets are compared against the ARP access list, and packets are permitted only if the access list permits them. If access lists deny packets because of explicit denies, they are dropped. If packets get denied because of the implicit deny, they are matched against the list of DHCP bindings, unless the access list is static or the packets are not compared against the bindings.

When an ARP access list is applied to a VLAN for dynamic ARP inspection, the ARP packets containing only IP-to-Ethernet MAC bindings are compared against the ACLs. All other packet types are bridged in the incoming VLAN without any validation.

ACL 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 ACL.

An implicit **deny any ip mac any** entry exists at the end of an ACL unless you include an explicit **permit ip any mac 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 new ARP ACL or enter the submode of an existing ARP ACL:

```
Router(config)# arp access-list arpacl22
Router(config-arp-nacl)#
```

This example shows how to create an ARP ACL named arp\_filtering that denies QoS but permits MAC-layer ARP traffic:

```
Router(config)# arp access-list arp_filtering
Router(config-arp-nacl)# permit ip host 1.1.1.1 mac any
Router(config-arp-nacl)# deny any ip mac any
Router(config-arp-nacl)#
```

### Related Commands

Command	Description
<a href="#">show arp</a>	Displays information about the ARP table.

# attach

To connect to a specific module from a remote location, use the **attach** command.

**attach** *num*

<b>Syntax Description</b>	<i>num</i> Module number; see the “Usage Guidelines” section for valid values.				
<b>Defaults</b>	This command has no default settings.				
<b>Command Modes</b>	Privileged EXEC				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(18)ZY</td> <td>Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)ZY	Support for this command was introduced.
Release	Modification				
12.2(18)ZY	Support for this command was introduced.				

## Usage Guidelines



### Caution

When you enter the **attach** or **remote login** command to access another console from your switch, if you enter global or interface configuration mode commands, the switch might reset.

The valid values for *num* depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values for the module number are from 1 to 13.

This command is supported on the supervisor engine only.

When you execute the **attach** *num* command, the prompt changes to Switch-sp#.

The **attach** command is identical to the **remote login module** *num* command.

There are two ways to end this session:

- You can enter the **exit** command as follows:

```
Switch-sp# exit
[Connection to Switch closed by foreign host]
Router#
```

- You can press **Ctrl-C** three times as follows:

```
Switch-sp# ^C
Switch-sp# ^C
Switch-sp# ^C
Terminate remote login session? [confirm] y
[Connection to Switch closed by local host]
Router#
```

---

**Examples**

This example shows how to log in remotely to the supervisor engine:

```
Router# attach 5
Trying Switch 111
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
Terminate remote login session? [confirm] yes
[Connection to Switch closed by local host]

Switch-sp#
```

---

**Related Commands**

Command	Description
<a href="#">remote login</a>	Accesses the Catalyst 6500 series switch console or a specific module.

# 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** | **running-config** | **standard** }

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

Syntax Description	Keyword	Description
	<b>startup-config</b>	Specifies the automatic synchronization of the startup configuration.
	<b>config-register</b>	Specifies the automatic synchronization of the configuration register configuration.
	<b>bootvar</b>	Specifies the automatic synchronization of the BOOTVAR configuration.
	<b>running-config</b>	Specifies the automatic synchronization of the running configuration.
	<b>standard</b>	Specifies the automatic synchronization of the startup-config, BOOTVAR, and configuration registers.

**Defaults** Automatic synchronization of the running configuration.

**Command Modes** Main-cpu redundancy

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** If you enter the **no auto-sync standard** command, no automatic synchronizations occur. If you want to enable any of the keywords, you have to enter the appropriate command for each keyword.

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

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

Related Commands	Command	Description
	<b>redundancy</b>	Enters redundancy configuration mode.

# bgp regexp deterministic

To configure Cisco IOS software to use the deterministic processing time regular expression engine, use the **bgp regexp deterministic** command. To configure Cisco IOS software to use the default regular expression engine, use the **no** form of this command.

**bgp regexp deterministic**

**no bgp regexp deterministic**

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

**Defaults** The default regular expression engine is enabled.

**Command Modes** Router configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The default Cisco IOS regular expression engine uses a recursive algorithm. This engine is effective but uses more system resources as the complexity of regular expressions increases. The recursive algorithm works well for simple regular expressions, but is less efficient when processing very complex regular expressions because of the backtracking that is required by the default engine to process partial matches. In some cases, CPU watchdog timeouts and stack overflow traces have occurred because of the length of time that the default engine requires to process very complex regular expressions.

The deterministic processing time regular expression engine does not replace the default regular expression engine. The new engine employs an improved algorithm that eliminates excessive backtracking and greatly improves performance when processing complex regular expressions. When the new engine is enabled, complex regular expressions are evaluated more quickly, and CPU watchdog timeouts and stack overflow traces will not occur. However, the new regular expression engine takes longer to process simple regular expressions than the default engine.

We recommend that you use the new regular expression engine if you need to evaluate complex regular expressions or if you have observed problems related to evaluating regular expressions. We recommend that you use the default regular expression engine if you use only simple regular expressions. The new engine can be enabled by entering the **bgp regexp deterministic** command under a BGP routing process. The default regular expression engine can be reenabled by entering the **no** form of this command.

---

**Examples**

This example shows how to configure Cisco IOS software to use the deterministic processing time regular expression engine:

```
Router(config)# router bgp 1  
Router(config-router)# bgp regexp deterministic  
Router(config-router)#
```

This example shows how to configure Cisco IOS software to use the default regular expression engine:

```
Router(config)# router bgp 1  
Router(config-router)# no bgp regexp deterministic  
Router(config-router)#
```

# boot config

To specify the device and filename of the configuration file from which the system configures itself during initialization (startup), use the **boot config** command. To remove the specification, use the **no** form of this command.

**boot config** {*device:file-name*}

**no boot config**

Syntax Description	
<i>device:</i>	Device identification; see the “Usage Guidelines” section for a list of the valid values.
<i>file-name</i>	Configuration filename.

**Defaults** The configuration file is located in NVRAM.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The valid values for *device:* are as follows:

- **disk0:**
  - One external CompactFlash Type II slot
  - Supports CompactFlash Type II flash PC cards
- **sup-bootdisk:**
  - Supervisor Engine 32 256-MB internal CompactFlash flash memory
  - From the Supervisor Engine 32 ROMMON, it is bootdisk:
- **bootdisk:**
  - PISA 256-MB internal CompactFlash flash memory
  - Not accessible from the Supervisor Engine 32 ROMMON

When you use the **boot config** command, you affect only the running configuration. You must save the environment variable setting to your startup configuration to place the information under ROM monitor control and to have the environment variable function as expected. Use the **copy system:running-config nvram:startup-config** command to save the environment variable from your running configuration to your startup configuration.

The software displays an error message and does not update the CONFIG\_FILE environment variable in the following situations:

- You specify **nvr** as the file system, and it contains only a distilled version of the configuration. (A distilled configuration does not contain access lists.)
- You specify a configuration file in the filename argument that does not exist or is not valid.

During initialization, the NVRAM configuration is used when the CONFIG\_FILE environment variable does not exist or when it is null (such as at a first-time startup). If the software detects a problem with NVRAM or the configuration it contains, the device enters setup mode.

When you use the **no** form of this command, the NVRAM configuration is used as the startup configuration.

You can view the contents of the BOOT, BOOTLDR, and the CONFIG\_FILE environment variables using the **show bootvar** command. This command displays the settings for these variables as they exist in the startup configuration as well as in the running configuration if a running configuration setting differs from a startup configuration setting.

### Examples

This example shows how to set the configuration file that is located in the internal flash memory to configure itself during initialization. The third line copies the specification to the startup configuration, ensuring that this specification takes effect upon the next reload.

```
Router (config)# boot config disk0:router-config
Router (config)# end
Router# copy system:running-config nvram:startup-config
Router#
```

### Related Commands

Command	Description
<b>copy system:running-config nvram:startup-config</b>	Saves the environment variable from the running configuration to the startup configuration.
<b>show bootvar</b>	Displays information about the BOOT environment variable.

# boot system

To specify the system image that loads at startup, use the **boot system** command. To remove the startup system image specification, use the **no** form of this command.

**boot system** *filename*

**boot system flash** [*flash-fs:*][*partition-number:*][*filename*]

**no boot system** [*filename*]

**no boot system flash** [*flash-fs:*][*partition-number:*][*filename*]

Syntax Description		
<i>filename</i>		Specifies the configuration filename of the system image to load at system startup.
<b>flash</b>		Boots from internal flash memory.
<i>flash-fs:</i>		(Optional) flash file system containing the system image to load at startup; valid values are <b>flash:</b> , <b>bootflash</b> , <b>slot0</b> , and <b>slot1</b> .
<i>partition-number:</i>		(Optional) Number of the flash memory partition that contains the system image to boot, specified by the optional <i>filename</i> argument.
<i>filename</i>		(Optional when used with the <b>boot system flash</b> command) Case-sensitive name of the system image to load at startup.

## Defaults

If you configure the switch to boot from a network server but do not specify a system image file with the **boot system** command, the switch uses the configuration register settings to determine the default system image filename. The switch forms the default boot filename by starting with the word *cisco* and then appending the octal equivalent of the boot field number in the configuration register, followed by a hyphen (-) and the processor type name (*ciscorn-cpu*). Refer to the appropriate hardware installation guide for details on the configuration register and default filename. See also the **config-register** or **confreg** command.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

This command will not work unless you set the **config-register** command properly.

TFTP boot is not supported on the Catalyst 6500 series switches.

If you do not enter the *ip-address* argument, this value defaults to the IP broadcast address of 255.255.255.255.

The colon is required when entering the *flash-fs:* argument.

If you omit all arguments that follow the **flash** keyword, the system searches the internal flash memory for the first bootable image.

When using the *partition-number:* argument, if you do not specify a filename, the route processor loads the first valid file in the specified partition of flash memory. This argument is valid only on route processors that can be partitioned.

The *filename* argument is case sensitive. If you do not specify a *filename*, the switch loads the first valid file in the following:

- The specified flash file system
- The specified partition of flash memory
- The default flash file system if you also omitted the *flash-fs:* argument

Enter several **boot system** commands to provide a fail-safe method for booting your route processor. The route processor stores and executes the **boot system** commands in the order in which you enter them in the configuration file. If you enter multiple boot commands of the same type (for example, if you enter two commands that instruct the route processor to boot from different network servers), the route processor tries them in the order in which they appear in the configuration file. If a **boot system** command entry in the list specifies an invalid device, the route processor omits that entry. Use the **boot system rom** command to specify use of the ROM system image as a backup to other **boot** commands in the configuration.

For some platforms, you must load the boot image before you load the system image. However, on many platforms, the boot image that you specify loads only if the route processor is booting from a network server or if you do not specify the flash file system. If you specify the file system, the route processor boots faster because it does not need to load the boot image first.

For detailed information, refer to the *Cisco IOS Release 12.2 Command Reference*.



#### Note

When you use the **boot system** command, you affect only the running configuration. You must save the BOOT variable settings to your startup configuration to place the information under ROM monitor control and to have the variable function as expected. Use the **copy system:running-config nvram:startup-config EXEC** command to save the variable from your running configuration to your startup configuration.

To view the contents of the BOOT variable, use the **show bootenv EXEC** command.

#### Examples

This example shows a system filename with the ROM software as a backup:

```
Router(config)# boot system flash config1
Router(config)# boot system rom
```

This example shows how to boot the system image filenameed igs-bpx-1 from partition 2 of the flash device:

```
Router(config)# boot system flash:2:igs-bpx-1
Router(config)#
```

Related Commands	Command	Description
	<b>config-register</b>	Changes the configuration register settings.
	<b>copy /noverify</b>	Disables the automatic image verification for the current copy operation.
	<b>ip rcmd remote username</b>	Configures the remote username to be used when requesting a remote copy using rcp.
	<b>show bootvar</b>	Displays information about the BOOT environment variable.

# bridge-domain

To enable BPDU translation, use the **bridge-domain** command.

**bridge-domain** {*vlan* | {*PE-vlan* **dot1qtunnel**}} [**ignore-bpdu-pid**] {**pvst-tlv** *CE-vlan*}

Syntax Description	
<i>vlan</i>	VLAN number on a back-to back topology.
<i>PE-vlan</i> <b>dot1qtunnel</b>	Specifies the provider-edge VLAN number on a Layer 2 topology.
<b>ignore-bpdu-pid</b>	(Optional) Sends out IEEE BPDUs using a PID of 0x00-07, which is normally reserved for RFC 1483 data.
<b>pvst-tlv</b>	When transmitting, translates PVST+ BPDUs into IEEE BPDUs. When receiving, translates IEEE BPDUs into PVST+ BPDUs.
<i>CE-vlan</i>	Customer-edge VLAN in the SSTP TLV to be inserted in an IEEE BPDU to a PVST+ BPDU conversion.

**Defaults** Disabled

**Command Modes** VC or DLCI configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The *CE-vlan* argument does not have to be the same as the *PE-vlan* argument.

When connecting to a device that is completely RFC-1483 compliant, in which the IEEE BPDUs are sent using a PID of 0x000E, you must use the **ignore-bpdu-pid** keywords in the **bridge-domain** command.

If you do not enter the **ignore-bpdu-pid** keyword, the PVC between the devices operates in an RFC-1483 compliant topology, which is referred to as *strict mode*. Entering the **ignore-bpdu-pid** keyword enters the *loose mode*. Both modes are described as follows:

- Without the **ignore-bpdu-pid** keywords, in strict mode, IEEE BPDUs are sent out using a PID of 0x00-0E, which complies with RFC 1483.
- With the **ignore-bpdu-pid** keywords, in loose mode, IEEE BPDUs are sent out using a PID of 0x00-07, which is normally reserved for RFC-1483 data.

Cisco-proprietary PVST+ BPDUs are always sent out on data frames using a PID of 0x00-07, regardless of whether you enter the **ignore-bpdu-pid** keywords.

Use the **ignore-bpdu-pid** keywords when connecting to devices (such as ATM DSL modems) that send PVST (or 802.1D) BPDUs with PID: 00-07.

The **pvst-tlv** keyword enables BPDU translation when interoperating with devices that understand only PVST or IEEE Spanning Tree Protocol. Because the Catalyst 6500 series switch ATM modules support PVST+ only, you must use the **pvst-tlv** keyword when connecting to a Catalyst 5000 family switch, which only understands PVST on its ATM modules, or when connecting with other Cisco IOS route processors, which understand IEEE format only.

When transmitting, the **pvst-tlv** keyword translates PVST+ BPDUs into IEEE BPDUs.

When receiving, the **pvst-tlv** keyword translates IEEE BPDUs into PVST+ BPDUs.

---

## Examples

This example shows how to enable BPDU translation when a Catalyst 6500 series switch is connected to a device that only understand IEEE BPDUs in an RFC-1483 compliant topology:

```
Router(config-if-atm-vc)# bridge-domain 100 pvst-tlv 150
Router(config-if-atm-vc)#
```

The **ignore-bpdu-pid** keyword is not used because the device operates in an RFC-1483 compliant topology for IEEE BPDUs.

This example shows how to enable BPDU translation when a Catalyst 5500 ATM module is a device that only understands PVST BPDUs in a non-RFC1483 compliant topology. When a Catalyst 6500 series switch is connected to a Catalyst 5500 ATM module, you must enter both keywords:

```
Router(config-if-atm-vc)# bridge-domain 100 ignore-bpdu-pid pvst-tlv 150
Router(config-if-atm-vc)#
```

To enable BPDU translation for the Layer 2 Protocol Tunneling (L2PT) topologies, use the following command line:

```
Router(config-if-atm-vc)# bridge-domain 100 dot1qtunnel ignore-bpdu-pid pvst-tlv 150
Router(config-if-atm-vc)#
```

# cd

To change the default directory or file system, use the **cd** command.

```
cd [filesystem:][directory]
```

<b>Syntax Description</b>	<i>filesystem:</i>	(Optional) URL or alias of the directory or file system that is followed by a colon; see the “Usage Guidelines” section for a list of the valid values.
	<i>directory</i>	(Optional) Name of the directory.

<b>Defaults</b>	Initial default file system is <b>disk0:</b>
-----------------	--

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	<p>The valid values for <i>filesystem:</i> are <b>bootflash:</b>, <b>disk0:</b> and <b>disk1:</b>.</p> <p>For all EXEC commands that have an optional <i>filesystem</i> argument, the system uses the file system that is specified by the <b>cd</b> command when you omit the optional <i>filesystem</i> argument. For example, the <b>dir</b> command, which displays a list of files on a file system, contains an optional <i>filesystem</i> argument. When you omit this argument, the system lists the files on the file system that is specified by the <b>cd</b> command.</p> <p>If you do not specify a directory on a file system, the default is the root directory on that file system.</p>
-------------------------	---

<b>Examples</b>	This example sets the default file system to the flash PC card that is inserted in disk 0:
-----------------	--

```
Router# cd disk0:
Router# pwd
disk0:/
```

Related Commands	Command	Description
	<b>dir</b>	Displays a list of files on a file system.
	<b>mkdir disk0:</b>	Creates a new directory in a flash file system.
	<b>pwd</b>	Displays the current setting of the <b>cd</b> command.
	<b>show file system</b>	Displays the available file systems.
	<b>undelete</b>	Recovers a file that is marked “deleted” on a flash file system.

# channel-group

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

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

**no channel-group** *number*

Syntax Description	<i>number</i>	Channel-group number; valid values are a maximum of 64 values ranging from 1 to 256.
	<b>mode</b>	Specifies the EtherChannel mode of the interface.
	<b>active</b>	Enables LACP unconditionally.
	<b>on</b>	Enables EtherChannel only.
	<b>auto</b>	Places a port into a passive negotiating state in which the port responds to PAgP packets that it receives but does not initiate PAgP packet negotiation.
	<b>non-silent</b>	(Optional) Used with the <b>auto</b> or <b>desirable</b> mode when traffic is expected from the other device.
	<b>desirable</b>	Places a port into an active negotiating state in which the port initiates negotiations with other ports by sending PAgP packets.
	<b>passive</b>	Enables LACP only if an LACP device is detected.

**Defaults** No channel groups are assigned.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines



### Note

You cannot make any changes to the configuration of the Supervisor Engine 32 PISA EtherChannel.



### Note

After the port becomes a member of the Supervisor Engine 32 PISA EtherChannel, only the **no channel-group 256 mode on** command has any effect on the port until the port is no longer a member of the PISA EtherChannel. While the port is a member of the PISA EtherChannel, all port configuration commands except the **no channel-group 256 mode on** command are ignored.

By default, the Supervisor Engine 32 PISA EtherChannel (port channel interface 256, which is automatically configured with the **pisa-channel** command) is a 1-Gps EtherChannel.

**Note**

The **pisa-channel** command is visible in the configuration file, but it is not user configurable.

The channel-group number is global and is shared between all the channeling protocols. If a specific channel number is used for the PAGP-enabled interfaces of a channel group, that same channel number cannot be used for configuring a channel that has LACP-enabled interfaces or vice versa.

Entering the **auto** or **desirable** keyword enables PAGP on the specified interface; the command will be rejected if it is issued on an LACP-enabled interface.

The **active** and **passive** keywords are valid on PAGP-disabled interfaces only.

You can change the mode for an interface only if it is the only interface that is designated to the specified channel group.

The **on** keyword forces the bundling of the interface on the channel without any negotiation.

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

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

If you enter the **channel group** command on an interface that is added to a channel with a different protocol than the protocol you are entering, the command is rejected.

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

All ports in the same channel group must use the same protocol; you cannot run two protocols on one channel group.

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

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.

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

You do not have to create a port-channel interface before assigning a physical interface to a channel group. A port-channel interface is created automatically when the channel group gets its first physical interface, if it is not already created.

You do not have to disable the IP address that is assigned to a physical interface that is part of a channel group, but it is highly recommended.

You can create both Layer 2 and Layer 3 port channels by entering the **interface port-channel** command or when the channel group gets its first physical interface assignment. The port channels are not created at runtime or dynamically.

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

When configuring Layer 2 EtherChannels, you cannot put Layer 2 LAN ports into manually created port-channel logical interfaces.

You cannot use the **channel-group** command on GE-WAN interfaces if MPLS is configured. You must remove all IP, MPLS, and other Layer 3 configuration commands before using the **channel-group** command with GE-WAN interfaces.

**Note**

You can enter the **channel-group** command again to delete the interface from the old group and move it to the new group. For GE-WAN ports, however, you must manually remove the interface from the group by entering the **no channel-group** command before assigning it to a new group.

**Caution**

Do not enable Layer 3 addresses on the physical EtherChannel interfaces. Assigning bridge groups on the physical EtherChannel interfaces causes loops in your network.

For a complete list of guidelines, refer to the “Configuring EtherChannel” section of the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*.

**Examples**

This example shows how to add EtherChannel interface 1/0 to the EtherChannel group that is specified by port-channel 1:

```
Router(config-if)# channel-group 1 mode on
Router(config-if)#
```

**Related Commands**

Command	Description
<a href="#">interface port-channel</a>	Creates a port-channel virtual interface and enters interface configuration mode.
<a href="#">show etherchannel</a>	Displays the EtherChannel information for a channel.
<a href="#">show interfaces port-channel</a>	Displays the traffic that is seen by a specific port channel.

# channel-protocol

To set the protocol that is used on an interface to manage channeling, use the **channel-protocol** command. To deselect the protocol, use the **no** form of this command.

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

**no channel-protocol**

Syntax Description	lacp	pagp
	Specifies LACP to manage channeling.	Specifies PAgP to manage channeling.

Defaults	pagp

Command Modes	Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

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

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

All ports in an EtherChannel must use the same protocol.

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

The **channel-protocol** command is performed on a channel-group basis and affects ports in the channel group that is being reconfigured only. You can use the **channel-protocol** command to restrict anyone from selecting a mode that is not applicable to the selected protocol.

Configure all ports in an EtherChannel to operate at the same speed and duplex mode (full duplex only for LACP mode). For a complete list of guidelines, refer to the “Configuring EtherChannel” section of the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*.

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

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

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

# class-map

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

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

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

Syntax Description	<i>name</i>	Class map name.
	<b>match-all</b>	(Optional) Matches all match criteria in the class map.
	<b>match-any</b>	(Optional) Matches one or more match criteria.

**Defaults** When you do not specify the **match-all** or **match-any** keyword, the default is **match-all**.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** You apply the **class-map** command and its subcommands on a per-interface basis to define packet classification, marking, aggregate, and flow policing as part of a globally named service policy. You can attach a service policy to an EtherChannel. Do not attach a service policy to a port that is a member of an EtherChannel.

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

- **exit**—Used to exit from QoS class map configuration mode.
- **no**—Used to remove a match statement from a class map.
- **match**—Used to configure classification criteria. These optional **match** subcommands are available:
  - **access-group** {*acl-index* | *acl-name*}
  - **ip** {**dscp** | **precedence**} *value1 value2 ... value8*

These subcommands appear in the CLI help but are not supported on LAN interfaces or WAN interfaces on the OSMs:

- **input-interface** {{*interface interface-number*} | {**null** *number*} | {**vlan** *vlan-id*}}
- **protocol** *linktype*
- **destination-address** **mac** *mac-address*
- **source-address** **mac** *mac-address*

PFC QoS does not support these subcommands:

- **input-interface** *{{ interface interface-number } | { null number } | { vlan vlan-id } }*
- **protocol** *linktype*
- **destination-address** **mac** *mac-address*
- **source-address** **mac** *mac-address*
- **qos-group** *group-value*

If you enter these subcommands, PFC QoS does not detect the unsupported keywords until you attach a policy map to an interface. When you try to attach the policy map to an interface, you get an error message. For additional information, refer to the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY* and the *Cisco IOS Release 12.2 Command Reference* publications.

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

```
match {{{access-group acl-index} | acl-name} | [{ip dscp} | {precedence value}]}}
```

See [Table 2-1](#) for a syntax description of the **match** subcommands.

**Table 2-1** match Syntax Description

Optional Subcommand	Description
<b>access-group</b> <i>acl-index</i> / <i>acl-name</i>	Specifies the access list index or access list names; valid access list index values are from 1 to 2699.
<b>access-group</b> <i>acl-name</i>	Specifies the named access list.
<b>ip dscp</b> <i>value1 value2 ... value8</i>	Specifies the IP DSCP values to match; valid values are from 0 to 63. You can enter up to 8 DSCP values, and separate each value with one white space.
<b>ip precedence</b> <i>value1 value2 ... value8</i>	Specifies the IP precedence values to match; valid values are from 0 to 7. You can enter up to 8 precedence values, and separate each value with one white space.

### Examples

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

```
Router(config)# class-map ipp5
Router(config-cmap)# match ip precedence 5
Router(config-cmap)#
```

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

```
Router(config-cmap)# match access-group IPac11
Router(config-cmap)#
```

### Related Commands

Command	Description
<a href="#">policy-map</a>	Accesses QoS policy-map configuration mode to configure the QoS policy map.
<a href="#">show class-map</a>	Displays class-map information.
<a href="#">show policy-map interface</a>	Displays the statistics and the configurations of the input and output policies that are attached to an interface.

## class-map type multicast-flows

To create multicast class maps and enter the multicast class map configuration mode, use the **class-map type multicast-flows** command. To delete a class map, use the **no** form of this command.

**class-map type multicast-flows** *name*

**no class-map type multicast-flows** *name*

Syntax Description	<i>name</i>	Class-map name.
--------------------	-------------	-----------------

Defaults	No class is specified.
----------	------------------------

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** After you are in the multicast class-map configuration mode, these configuration commands are available:

- **exit**—Used to exit from multicast class-map configuration mode.
- **group**—Used to configure a multicast group range. The syntax for these subcommands is as follows:

**group** *group-addr* [**source** *addr* | **to** *addr*]

See [Table 2-2](#) for a syntax description of the **group** subcommands.

**Table 2-2** *group Syntax Description*

Subcommand	Description
<i>group-addr</i>	Multicast group address.
<b>source</b> <i>addr</i>	(Optional) Specifies the channel-source address.
<b>to</b> <i>addr</i>	(Optional) Specifies the multicast group range end address.

- **no**—Used to negate a command or set its defaults.

## Examples

This example shows how to create a multicast class map:

```
Router(config)# class-map type multicast-flows static2
Router(config-mcast-flows-cmap)#
```

This example shows how to configure a multicast group range:

```
Router(config-mcast-flows-cmap)# group 192.0.2.0 source 192.0.2.10
Router(config-mcast-flows-cmap)#
```

## class (policy-map)

To specify the name of the class that has a policy that you want to create or change or to specify the default class (commonly known as the class-default class) before you configure its policy, use the **class** command in QoS policy-map configuration mode. To remove a class from the policy map, use the **no** form of this command.

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

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

### Syntax Description

<i>class-name</i>	Name of the class to configure or modify the policy.
<b>class-default</b>	Specifies the default class.

### Defaults

No class is specified.

### Command Modes

QoS policy-map configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

You can use the **class** (policy-map) command to specify the class name of the policy that you want to create or change. You must first identify the policy map.

To identify the policy map (and enter the required QoS policy-map configuration mode), use the **policy-map** command before you use the **class** (policy-map) command. After you specify a policy map, you can configure the policy for new classes or modify the policy for any existing classes in that policy map.

To define the class characteristics, use the following guidelines:

- The class name that you specify in the policy map ties the characteristics for that class—that is, its policy—to the class map and its match criteria, as configured using the **class-map** command.
- When you configure a policy for a class, specify its bandwidth, and attach the policy map to an interface, CBWFQ determines if the bandwidth requirement of the class can be satisfied. If so, CBWFQ allocates a queue for the bandwidth requirement.
- When a class is removed, available bandwidth for the interface is incremented by the amount that was previously allocated to the class.
- The maximum number of classes that you can configure within a policy map is 64.

The **class-default** keywords are used to specify the predefined default class called class-default. The predefined default class called class-default is the class to which traffic is directed if that traffic does not match any of the match criteria in the configured class maps.

You can define a class policy to use either tail drop by using the **queue-limit** command or WRED by using the **random-detect** command. When using either tail drop or WRED, follow these guidelines:

- The **queue-limit** and **random-detect** commands cannot be used in the same class policy, but they can be used in two class policies in the same policy map.
- You can use the **bandwidth** command when either the **queue-limit** or the **random-detect** command is configured in a class policy. The **bandwidth** command specifies the amount of bandwidth allocated for the class.
- For the predefined default class, you can use the **fair-queue** (class-default) command. The **fair-queue** command specifies the number of dynamic queues for the default class. The **fair-queue** command can be used in the same class policy as either the **queue-limit** or **random-detect** command; it cannot be used with the **bandwidth** command.

## Examples

This example shows how to configure three class policies included in the policy map called policy1. Class1 specifies the policy for the traffic that matches access control list 136. Class2 specifies the policy for the traffic on interface ethernet101. The third class is the default class to which packets that do not satisfy configured match criteria are directed.

```
Router(config)# policy-map policy1
Router(config-pmap)# class-map class1
Router(config-pmap-c)# match access-group 136
Router(config-pmap)# class-map class2
Router(config-pmap-c)# match input-interface ethernet101
```

These examples show how to create the policy map that contains the policy specifications for class1, class2, and the default class:

```
Router(config)# policy-map policy1
Router(config-pmap)# class-map class1
Router(config-pmap-c)# bandwidth 2000
Router(config-pmap-c)# queue-limit 40

Router(config-pmap)# class class2
Router(config-pmap-c)# bandwidth 3000
Router(config-pmap-c)# random-detect
Router(config-pmap-c)# random-detect exponential-weighting-constant 10

Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue 16
Router(config-pmap-c)# queue-limit 20
```



### Note

When the policy map containing these classes is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed, including all class policies and the Resource Reservation Protocol (RSVP), if configured.

This example shows how to configure the policy for the **class-default** default class included in the policy map called policy8. The **class-default** default class has 20 hashed queues for the traffic that does not meet the match criteria of the other classes that have policies that are defined by the policy map called policy8 and a weight factor of 14 that is used to calculate the average queue size. For congestion avoidance, WRED packet drop is used, not tail drop.

```
Router(config)# policy-map policy8
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue 20
Router(config-pmap-c)# random-detect exponential-weighting-constant 14
```

Related Commands	Command	Description
	<b>class-map</b>	Accesses the QoS class map configuration mode to configure QoS class maps.
	<b>fair-queue</b>	Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy.
	<b>policy-map</b>	Accesses the QoS policy-map configuration mode to configure the QoS policy map.
	<b>queue-limit</b>	Specifies or modifies the maximum number of packets that the queue can hold for a class policy configured in a policy map.
	<b>random-detect (interface)</b>	Enables WRED or DWRED.
	<b>random-detect exponential-weighting-constant</b>	Configures the WRED and DWRED exponential weight factor for the average queue size calculation for the queue.
	<b>random-detect precedence</b>	Configures the WRED and DWRED parameters for a particular IP precedence.

# clear cable-diagnostics tdr

To clear a specific interface or clear all interfaces that support time domain reflectometry (TDR), use the **clear cable-diagnostics tdr** command.

**clear cable-diagnostics tdr** [**interface** *interface interface-number*]

<b>Syntax Description</b>	<b>interface</b> <i>interface</i> (Optional) Specifies the interface type; possible valid values are <b>fastethernet</b> , <b>gigabitethernet</b> , and <b>tengigabitethernet</b> .
	<i>interface-number</i> Module and port number; see the “Usage Guidelines” section for valid values.

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

**Command Modes** Privileged EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** See the *Release Notes for Cisco IOS Release 12.2 SX on the Catalyst 6500* for the list of modules that support TDR.

**Examples** This example shows how to clear a specific interface:

```
Router# clear cable-diagnostics tdr interface gigabitethernet 4/1
Router#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show cable-diagnostics tdr</a>	Displays the test results for the TDR cable diagnostics.
	<a href="#">test cable-diagnostics</a>	Tests the condition of 10-Gigabit Ethernet links or copper cables on 48-port 10/100/1000 BASE-T modules.

# clear catalyst6000 traffic-meter

To clear the traffic meter counters, use the **clear catalyst6000 traffic-meter** command.

**clear catalyst6000 traffic-meter**

---

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

---

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

---

**Command Modes** Privileged EXEC

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Examples** This example shows how to clear the traffic meter counters:

```
Router# clear catalyst6000 traffic-meter
Router#
```

# clear counters

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

```
clear counters [{interface interface-number} | {null interface-number} | {port-channel number}
| {vlan vlan-id}]
```

Syntax Description		
<i>interface</i>	(Optional) Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , and <b>tengigabitethernet</b> . See the “Usage Guidelines” section for additional valid values.	
<i>interface-number</i>	(Optional) Module and port number; see the “Usage Guidelines” section for valid values.	
<b>null</b> <i>interface-number</i>	(Optional) Specifies the null interface; the valid value is <b>0</b> .	
<b>port-channel</b> <i>number</i>	(Optional) Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 256.	
<b>vlan</b> <i>vlan-id</i>	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.	

## Defaults

This command has no default settings.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

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



### Note

This command does not clear counters that are retrieved using SNMP but only those counters that appear when you enter the **show queueing interface** command.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

**Examples**

This example shows how to clear all interface counters:

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

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

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

**Related Commands**

Command	Description
<a href="#">show queueing interface</a>	Displays queueing information.

# clear fm netflow counters

To clear the NetFlow counters, use the **clear fm netflow counters** command.

**clear fm netflow counters**

---

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

---

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

---

**Command Modes** Privileged EXEC

---

Release	Modification
12.2(18)ZY	Support for this command was introduced.

---

---

**Examples** This example shows how to clear the NetFlow counters:

```
Router# clear fm netflow counters
Router#
```

# clear interface gigabitethernet

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

**clear interface gigabitethernet** *number*

## Syntax Description

<i>number</i>	Gigabit Ethernet interface number; see the “Usage Guidelines” section for valid values.
---------------	---

## Defaults

This command has no default settings.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

The *number* argument designates the module and port number. Valid values for *number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

## Examples

This example shows how to clear the hardware logic on a Gigabit Ethernet IEEE 802.3z interface:

```
Router# clear interface gigabitethernet 5
Router#
```

## Related Commands

Command	Description
<a href="#">show interfaces status</a>	Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.

# clear interface vlan

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

**clear interface vlan** *vlan-id*

<b>Syntax Description</b>	<i>vlan-id</i> VLAN ID; valid values are from 1 to 4094.				
<b>Defaults</b>	This command has no default settings.				
<b>Command Modes</b>	Privileged EXEC				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(18)ZY</td> <td>Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)ZY	Support for this command was introduced.
Release	Modification				
12.2(18)ZY	Support for this command was introduced.				
<b>Examples</b>	<p>This example shows how to clear the hardware logic on a specific VLAN:</p> <pre>Router# clear interface vlan 5 Router#</pre>				
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><a href="#">show interfaces status</a></td> <td>Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.</td> </tr> </tbody> </table>	Command	Description	<a href="#">show interfaces status</a>	Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.
Command	Description				
<a href="#">show interfaces status</a>	Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.				

# clear ip access-template

To clear statistical information on the access list, use the **clear ip access-template** command.

**clear ip access-template** *access-list*

<b>Syntax Description</b>	<i>access-list</i> Access list number; 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.
---------------------------	---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to clear statistical information on the access list:

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show mls netflow</a>	Displays configuration information about the NetFlow hardware.

# clear ip arp inspection log

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

## clear ip arp inspection log

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

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

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

```
Router# clear ip arp inspection log
Router#
```

Related Commands	Command	Description
	<a href="#">arp access-list</a>	Configures an ARP ACL for ARP inspection and QoS filtering and enters the ARP ACL configuration submode.
	<a href="#">show ip arp inspection log</a>	Displays the status of the log buffer.

# clear ip arp inspection statistics

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

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

<b>Syntax Description</b>	<b>vlan</b> <i>vlan-range</i> (Optional) Specifies the VLAN range.
---------------------------	--

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

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

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">arp access-list</a>	Configures an ARP ACL for ARP inspection and QoS filtering and enters the ARP ACL configuration submode.
	<a href="#">clear ip arp inspection log</a>	Clears the status of the log buffer.
	<a href="#">show ip arp inspection log</a>	Displays the status of the log buffer.

# clear ip auth-proxy watch-list

To delete a single watch-list entry or all watch-list entries, use the **clear ip auth-proxy watch-list** command.

```
clear ip auth-proxy watch-list {ip-addr | *}
```

Syntax Description	<i>ip-addr</i>	IP address to be deleted from the watch list.
	*	All watch-list entries from the watch list.

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

**Command Modes** Privileged EXEC.

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** If you see entries in the watch list that you suspect are not valid, you can enter the **clear ip auth-proxy watch-list** command to clear them manually instead of waiting for the watch list to expire.

**Examples** This example shows how to delete a single watch-list entry:

```
Router# clear ip auth-proxy watch-list 12.0.0.2
Router#
```

This example shows how to delete all watch-list entries:

```
Router# clear ip auth-proxy watch-list *
Router#
```

Related Commands	Command	Description
	<a href="#">ip auth-proxy max-login-attempts</a>	Limits the number of login attempts at a firewall interface and QoS filtering and enters the ARP ACL configuration submenu.
	<a href="#">ip auth-proxy watch-list</a>	Enables and configures an authentication proxy watch list.
	<a href="#">show ip auth-proxy watch-list</a>	Displays the information about the authentication proxy watch list.

# clear ip cef epoch full

To begin a new epoch and increment the epoch number for all tables (including the adjacency table), use the **clear ip cef epoch full** command.

## clear ip cef epoch full

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

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Use the **clear ip cef epoch full** command when you want to rebuild a table. This command allows old and new table entries to be distinguished within the same data structure and allows you to retain the old CEF database table while constructing the new table.

These **show** commands display epoch information:

- **show ip cef summary**—Displays the table epoch for a specific FIB table.
- **show ip cef detail**—Displays the epoch value for each entry of a specific FIB table.
- **show adjacency summary**—Displays the adjacency table epoch.
- **show adjacency detail**—Displays the epoch value for each entry of the adjacency table.

**Examples** This example shows the output before and after you clear the epoch table and increment the epoch number:

```
Router# show ip cef epoch
CEF epoch information:

Table:Default-table
  Table epoch:5 (464 entries at this epoch)

Adjacency table
  Table epoch:4 (33 entries at this epoch)
```

```

Router# clear ip cef epoch full
Router# show ip cef epoch
CEF epoch information:

Table:Default-table
  Table epoch:3 (464 entries at this epoch)

Adjacency table
  Table epoch:5 (33 entries at this epoch)
Router#

```

---

**Related Commands**

Command	Description
<b>show adjacency detail</b>	Displays the information about the protocol detail and timer.
<b>show adjacency summary</b>	Displays a summary of CEF-adjacency information.
<b>show ip cef detail</b>	Displays detailed FIB entry information.
<b>show ip cef epoch</b>	Displays the epoch information for the adjacency table and all FIB tables.
<b>show ip cef summary</b>	Displays a summary of the FIB.

# clear ip cef inconsistency

To clear the statistics and records for the CEF-consistency checker, use the **clear ip cef inconsistency** command.

## clear ip cef inconsistency

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

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command clears the statistics and records that accumulate when you enable the **ip cef table consistency-check** command.

**Examples** This example shows how to clear all statistics and records for the CEF-consistency checker:

```
Router# clear ip cef inconsistency
Router#
```

Related Commands	Command	Description
	<b>ip cef table consistency-check</b>	Enables the CEF-table consistency-checker types and parameters.

# clear ip dhcp snooping

To clear the DHCP-snooping table without disabling DHCP snooping, use the **clear ip dhcp snooping** command.

**clear ip dhcp snooping** { **binding** | **database** | **statistics** }

Syntax Description	binding	Clears the DHCP-snooping binding-entry table without disabling DHCP snooping.
	<b>database</b>	Clears the DHCP-snooping database table without disabling DHCP snooping.
	<b>statistics</b>	Clears the DHCP-snooping statistics table without disabling DHCP snooping.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to clear the DHCP-snooping binding-entry table:

```
Router# clear ip dhcp snooping binding
Router#
```

This example shows how to clear the DHCP-snooping database table:

```
Router# clear ip dhcp snooping database
Router#
```

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

```
Router# clear ip dhcp snooping statistics
Router#
```

Related Commands	Command	Description
	<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.
	<a href="#">show ip dhcp snooping binding</a>	Displays the DHCP snooping binding entries.
	<a href="#">show ip dhcp snooping database</a>	Displays the status of the DHCP snooping database agent.

# clear ip flow stats

To clear the NetFlow-switching statistics, use the **clear ip flow stats** command.

## clear ip flow stats

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

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **show ip cache flow** command displays the NetFlow-switching statistics.

**Examples** This example shows how to clear the NetFlow-switching statistics:

```
Router# clear ip flow stats
Router#
```

Related Commands	Command	Description
	<b>show ip cache flow</b>	Displays a summary of the NetFlow cache-flow entries.

# clear ip igmp group

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

```
clear ip igmp [vrf vrf-name] group [{interface interface-number} | {group-name | group-address}
  {loopback interface-number} | {null interface-number} | {port-channel number} |
  {vlan vlan-id}]
```

Syntax Description	
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
<i>interface</i>	(Optional) Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , and <b>tengigabitethernet</b> .
<i>interface-number</i>	(Optional) Module and port number; see the “Usage Guidelines” section for valid values.
<i>group-name</i>	(Optional) Group name as defined in the DNS hosts table or with the <b>ip host</b> command.
<i>group-address</i>	(Optional) Address of the multicast group in four-part, dotted notation.
<b>loopback</b> <i>interface-number</i>	(Optional) Specifies the loopback interface; valid values are from 0 to 2147483647.
<b>null</b> <i>interface-number</i>	(Optional) Specifies the null interface; the valid value is <b>0</b> .
<b>port-channel</b> <i>number</i>	(Optional) Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 256.
<b>vlan</b> <i>vlan-id</i>	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The IGMP cache contains a list of hosts on the directly connected LAN. If the switch has joined a group, that group is also listed in the cache.

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

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

## ■ clear ip igmp group

**Examples**

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

```
Router# clear ip igmp group 224.0.255.1
Router#
```

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

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

**Related Commands**

Command	Description
<b>ip host</b>	Defines a static host name-to-address mapping in the host cache.
<b>show ip igmp groups</b>	Displays the multicast groups with receivers that are directly connected to the router and that were learned through IGMP.
<b>show ip igmp interface</b>	Displays the information about the IGMP-interface status and configuration.

# clear ip igmp snooping statistics

To clear the IGMP-snooping statistics, use the **clear ip igmp snooping statistics** command.

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

<b>Syntax Description</b>	<b>vlan</b> <i>vlan-id</i> (Optional) Specifies the VLAN ID; valid values are from 1 to 4094.
---------------------------	---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	If you do not enter a VLAN, the IGMP-snooping statistics for all VLANs is cleared.
-------------------------	--

<b>Examples</b>	This example shows how to clear the IGMP-snooping statistics for all VLANs:
-----------------	---

```
Router# clear ip igmp snooping statistics
Router#
```

This example shows how to clear the IGMP-snooping statistics for a specific VLAN:

```
Router# clear ip igmp snooping statistics vlan 300
Router#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show ip igmp snooping statistics</a>	Displays information about IGMPv3 statistics.

# clear ip mroute

To delete entries from the IP multicast routing table, use the **clear ip mroute** command.

```
clear ip mroute [vrf vrf-name] [* | group] [source]
```

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
*	Deletes all entries from the IP multicast routing table.	
<i>group</i>	Name or IP address of the multicast group; see the “Usage Guidelines” section for additional information.	
<i>source</i>	(Optional) Name or address of a multicast source that is sending to the group; see the “Usage Guidelines” section for additional information.	

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The *group* argument specifies one of the following:

- Name of the multicast group as defined in the DNS hosts table or with the **ip host** command.
- IP address of the multicast group in four-part, dotted notation.

If you specify a *group* name or address, you can also enter the *source* argument to specify a name or address of a multicast source that is sending to the group. A source does not need to be a member of the group.

**Examples** This example shows how to delete all entries from the IP multicast routing table:

```
Router# clear ip mroute *
Router#
```

This example shows how to delete all sources on the 228.3.0.0 subnet that are sending to the multicast group 224.2.205.42 from the IP multicast routing table. This example shows how to delete all sources on network 228.3, not individual sources:

```
Router# clear ip mroute 224.2.205.42 228.3.0.0
Router#
```

Related Commands	Command	Description
	<b>ip host</b>	Defines a static host name-to-address mapping in the host cache.
	<b>show ip mroute</b>	Displays the information about the IP-multicast routing table.

# clear ip msdp peer

To clear the TCP connection to the specified MSDP peer, use the **clear ip msdp peer** command.

```
clear ip msdp [vrf vrf-name] peer {peer-address | peer-name}
```

Syntax Description	<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
	<i>peer-address</i>   <i>peer-name</i>	IP address or name of the MSDP peer to which the TCP connection is cleared.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command closes the TCP connection to the peer, resets all the MSDP peer statistics, and clears the input and output queues to and from the MSDP peer.

**Examples** This example shows how to clear the TCP connection to the MSDP peer at 224.15.9.8:

```
Router# clear ip msdp peer 224.15.9.8
Router#
```

Related Commands	Command	Description
	<a href="#">ip msdp peer</a>	Configures an MSDP peer.

# clear ip msdp sa-cache

To clear MSDP source active cache entries, use the **clear ip msdp sa-cache** command.

**clear ip msdp** [*vrf vrf-name*] **sa-cache** [*group-address* | *group-name*]

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
<i>group-address</i>   <i>group-name</i>	(Optional) Multicast group address or name for which source active entries are cleared from the source active cache.	

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** In order to have any source active entries in the cache to clear, you must enable source active caching by entering the **ip msdp cache-sa-state** command.

If no multicast group is identified by group address or name, all source active cache entries are cleared.

**Examples** This example shows how to clear the source active entries for the multicast group 224.5.6.7 from the cache:

```
Router# clear ip msdp sa-cache 224.5.6.7
Router#
```

Related Commands	Command	Description
	<a href="#">ip msdp peer</a>	Configures an MSDP peer.
	<a href="#">ip msdp cache-sa-state</a>	Creates a source-active state on the router.
	<a href="#">show ip msdp sa-cache</a>	Displays (S, G) state learned from MSDP peers.

## clear ip msdp statistics

To clear statistics counters for one or all of the MSDP peers without resetting the sessions, use the **clear ip msdp statistics** command.

```
clear ip msdp [vrf vrf-name] statistics [peer-address | peer-name]
```

### Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
<i>peer-address</i>   <i>peer-name</i>	(Optional) Address or name of the MSDP peers whose statistics counters, reset count, and input/output count are cleared.

### Defaults

This command has no default settings.

### Command Modes

Privileged EXEC

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Examples

This example shows how to clear the counters for the peer named sanjose:

```
Router# clear ip msdp statistics sanjose
Router#
```

### Related Commands

Command	Description
<b>show ip msdp sa-cache</b>	Displays (S, G) state learned from MSDP peers.

# clear ip pim auto-rp

To delete entries from the Auto-RP cache, use the **clear ip pim auto-rp** command.

**clear ip pim** [*vrf vrf-name*] **auto-rp** *rp-address*

Syntax Description	Parameter	Description
	<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
	<i>rp-address</i>	Rendezvous-point address; see the “Usage Guidelines” section for additional information.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** When you enter the *rp-address* argument, only the entries related to the rendezvous point at this address are cleared. If you omit this argument, the entire Auto-RP cache is cleared.

**Examples** This example shows how to delete all entries from the Auto-RP cache:

```
Router# clear ip pim auto-rp 224.5.6.7
Router#
```

Related Commands	Command	Description
	<a href="#">show ip pim rp mapping</a>	Displays the mappings for the PIM group to the active rendezvous points.

# clear ip pim snooping statistics

To delete the IP PIM-snooping global statistics, use the **clear ip pim snooping statistics** command.

**clear ip pim snooping statistics**

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

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to clear the IP PIM statistics:

```
Router# clear ip pim snooping statistics
Router#
```

Related Commands	Command	Description
	<a href="#">ip pim snooping (global configuration mode)</a>	Enables PIM snooping globally.
	<a href="#">show ip pim snooping statistics</a>	Displays statistical information about IP PIM snooping.

# clear ip pim snooping vlan

To delete the IP PIM-snooping entries on a specific VLAN, use the **clear ip pim snooping vlan** command.

```
clear ip pim snooping vlan vlan-id mac-address gda-address
```

```
clear ip pim snooping vlan vlan-id mroute { * | { group-addr src-addr } { { downstream-neighbor ip-addr } | { upstream-neighbor ip-addr } } }
```

```
clear ip pim snooping vlan vlan-id neighbor { * | ip-addr }
```

Syntax Description		
<i>vlan-id</i>		VLAN ID; valid values are from 1 to 4094.
<b>mac-address</b> <i>gda-address</i>		Specifies the multicast group MAC address to delete.
<b>mroute</b> *		Deletes all mroute entries.
<b>mroute</b> <i>group-addr</i> <i>src-addr</i>		Deletes the mroute entries at the specified group and source IP address.
<b>downstream-neighbor</b> <i>ip-addr</i>		Deletes the entries at the specified downstream neighbor originating the join/prune message.
<b>upstream-neighbor</b> <i>ip-addr</i>		Deletes the entries at the specified upstream neighbor receiving the join/prune message.
<b>neighbor</b> *		Deletes all neighbors.
<b>neighbor</b> <i>ip-addr</i>		Deletes the neighbor at the specified IP address.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to clear the IP PIM statistics on a specific VLAN:

```
Router# clear ip pim snooping vlan 25 statistics
Router#
```

■ clear ip pim snooping vlan

Related Commands	Command	Description
	<a href="#">ip pim snooping (interface configuration mode)</a>	Enables PIM snooping on a specific interface.
	<a href="#">show ip pim snooping</a>	Displays information about IP PIM snooping.

# clear lacp counters

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

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

<b>Syntax Description</b>	<i>channel-group</i> (Optional) Channel group number; valid values are from 1 to 256.
---------------------------	---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	If you do not specify a <i>channel-group</i> , all channel groups are cleared.
	If you enter this command for a channel group that contains members in PAgP mode, the command is ignored.

<b>Examples</b>	This example shows how to clear the statistics for a specific group:
-----------------	--

```
Router# clear lacp 1 counters
Router#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show lacp</a>	Displays LACP information.

# clear logging ip access-list cache

To clear all the entries from the OAL cache and send them to the syslog, use the **clear logging ip access-list cache** command.

## clear logging ip access-list cache

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

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to clear all the entries from the OAL cache and send them to the syslog:

```
Router# clear logging ip access-list cache
Router#
```

Related Commands	Command	Description
	<a href="#">logging ip access-list cache (global configuration mode)</a>	Configures the OAL parameters globally.
	<a href="#">logging ip access-list cache (interface configuration mode)</a>	Enables an OAL-logging cache on an interface that is based on direction.
	<a href="#">show logging ip access-list</a>	Displays information about the logging IP access list.

# clear mac-address-table dynamic

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

```
clear mac-address-table dynamic [{address mac-addr} | {interface interface interface-number}
| {protocol {assigned | ip | ipx | other}}] [vlan vlan-id]
```

Syntax Description	
<b>address</b> <i>mac-addr</i>	(Optional) Specifies the MAC address.
<b>interface</b> <i>interface</i>	(Optional) Specifies the interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , and <b>tengigabitethernet</b> . See the “Usage Guidelines” section for additional valid values.
<i>interface-number</i>	(Optional) Module and port number; see the “Usage Guidelines” section for valid values.
<b>protocol assigned</b>	(Optional) Specifies the assigned protocol bucket accounts for such protocols as DECnet, Banyan VINES, and AppleTalk.
<b>protocol ip</b>   <b>ipx</b>	(Optional) Specifies the protocol type of the entries to clear.
<b>protocol other</b>	(Optional) Specifies the protocol types (other than IP or IPX) of the entries to clear.
<b>vlan</b> <i>vlan-id</i>	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

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

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

## ■ clear mac-address-table dynamic

**Examples**

This example shows how to clear all dynamic Layer 2 entries for a specific interface (e2/1) and protocol type (IPX):

```
Router# clear mac-address-table dynamic interface e2/1 protocol ipx
Router#
```

**Related Commands**

Command	Description
<a href="#">mac-address-table aging-time</a>	Configures the aging time for entries in the Layer 2 table.
<a href="#">mac-address-table static</a>	Adds static entries to the MAC-address table or configures a static MAC address with IGMP snooping disabled for that address.
<a href="#">show mac-address-table</a>	Displays the information about the MAC-address table.

# clear mls acl counters

To clear the MLS ACL counters, use the **clear mls acl counters** command.

```
clear mls acl counters { all | { interface interface interface-number } [ { loopback interface-number }
| { null interface-number } | { port-channel number } | { vlan vlan-id } ] }
```

Syntax Description		
<b>all</b>		Clears all the MLS ACL counters for all interfaces.
<b>interface</b> <i>interface</i>		Clears counters that are associated with the specified interface; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabithernet</b> , and <b>tengigabithernet</b> . See the “Usage Guidelines” section for additional valid values.
<i>interface-number</i>		Module and port number; see the “Usage Guidelines” section for valid values.
<b>loopback</b> <i>interface-number</i>	(Optional)	Specifies the loopback interface; valid values are from 0 to 2147483647.
<b>null</b> <i>interface-number</i>	(Optional)	Specifies the null interface; the valid value is <b>0</b> .
<b>port-channel</b> <i>number</i>	(Optional)	Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 256.
<b>vlan</b> <i>vlan-id</i>	(Optional)	Specifies the VLAN ID; valid values are from 1 to 4094.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** If you enter the **clear mls acl counters all**, all the MLS ACL counters for all the modules and the supervisor engines are cleared.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

**Examples** This example shows how to reset the MLS ACL counters in all interfaces:

```
Router# clear mls acl counters all
Router#
```

■ clear mls acl counters

Related Commands	Command	Description
	<a href="#">show tcam interface</a>	Displays information about the interface-based TCAM.

# clear mls cef ip accounting per-prefix

To clear information about the IP per-prefix accounting statistics, use the **clear mls cef ip accounting per-prefix** command.

```
clear mls cef ip accounting per-prefix {all | {prefix mask [instance]}}
```

Syntax Description	all	Clears all per-prefix accounting statistics information.
	<i>prefix</i>	Entry prefix in the format A.B.C.D.
	<i>mask</i>	Entry prefix mask.
	<i>instance</i>	(Optional) VPN Routing/Forwarding instance name.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to clear all information about the per-prefix accounting statistics:

```
Router# clear mls cef ip accounting per-prefix all
Router#
```

## clear mls cef ipv6 accounting per-prefix

To clear information about the IPv6 per-prefix accounting statistics, use the **clear mls cef ipv6 accounting per-prefix** command.

```
clear mls cef ipv6 accounting per-prefix {all | {ipv6-address/mask [instance]}}
```

Syntax Description	all	Clears all per-prefix accounting statistics information.
	<i>ipv6-address</i>	Entry IPv6 address; see the “Usage Guidelines” section for formatting information.
	<i>mask</i>	Entry prefix mask.
	<i>instance</i>	(Optional) VPN Routing/Forwarding instance name.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** When entering the *ipv6-address/mask* arguments, use this format, X:X:X:X::X/*mask*, where the valid values for *mask* are from 0 to 128.

**Examples** This example shows how to clear all information about the per-prefix accounting statistics:

```
Router# clear mls cef ipv6 accounting per-prefix all
Router#
```

# clear mls ip multicast bidir-rpcache

To clear all bidirectional (Bider) rendezvous-point cache entries, use the **clear mls ip multicast bidir-rpcache** command.

**clear mls ip multicast bidir-rpcache**

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

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to reset the Bidir counters:

```
Router# clear mls ip multicast bidir-rpcache
Router#
```

Related Commands	Command	Description
	<a href="#">show mls ip multicast bidir</a>	Displays the Bidir hardware-switched entries.

# clear mls ip multicast group

To delete an IP multicast group, use the **clear mls ip multicast group** command.

**clear mls ip multicast group** {*ip-name* | *group-address*}

Syntax Description	<i>ip-name</i>	Host IP name.
	<i>group-address</i>	(Optional) Address of the multicast group in four-part, dotted notation.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to delete an IP multicast group:

```
Router# clear mls ip multicast group 224.0.255.1
Router#
```

Related Commands	Command	Description
	<a href="#">show mls ip multicast group</a>	Displays the entries for a specific multicast-group address.

# clear mls ip multicast statistics

To reset the IP-multicast statistics counters, use the **clear mls ip multicast statistics** command.

**clear mls ip multicast statistics**

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

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to reset the IP-multicast statistics counters:

```
Router# clear mls ip multicast statistics
Router#
```

Related Commands	Command	Description
	<a href="#">show mls ip multicast</a>	Displays the MLS IP information.

# clear mls nde flow counters

To clear the NDE counters, use the **clear mls nde flow counters** command.

**clear mls nde flow counters**

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

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to reset the NDE counters:

```
Router# clear mls nde flow counters
Router#
```

Related Commands	Command	Description
	<a href="#">show mls nde</a>	Displays information about the NDE hardware-switched flow.

# clear mls netflow

To clear the MLS NetFlow-shortcut entries, use the **clear mls netflow** command.

```
clear mls netflow ip [destination ip-addr [source ip-addr-spec]] [dynamic | {sw-installed
non-static | static}] [module mod]
```

```
clear mls netflow ipv6 [destination ipv6-addr [ipv6-prefix] [source ipv6-addr [ipv6-prefix]]]
[flow {tcp | udp}] [{destination | source} port-num] [dynamic | {sw-installed [non-static |
static}] [module mod]
```

```
clear mls netflow mpls [top-label entry] [dynamic | {sw-installed [non-static | static}]
[module mod]
```

```
clear mls ipx [[module mod] [destination ipx-network [ipx-node]] [source ipx-network]
[macs mac-addr] [macd mac-addr] [interface interface-num] | [all]]
```

## Syntax Description

<b>ip</b>	Clears IP MLS entries.
<b>destination</b> <i>ip-addr</i>	(Optional) Specifies a destination full IP address or a subnet address. See the “Usage Guidelines” section for formatting guidelines.
<b>source</b> <i>ip-addr-spec</i>	(Optional) Specifies a source full IP address or a subnet address. See the “Usage Guidelines” section for formatting guidelines.
<b>dynamic</b>	(Optional) Clears NetFlow-statistics entries that are created in the hardware.
<b>sw-installed</b> <b>non-static</b>	(Optional) Clears software-installed nonstatic entries.
<b>sw-installed</b> <b>static</b>	(Optional) Clears software-installed static entries.
<b>module</b> <i>mod</i>	(Optional) Specifies a module number.
<b>ipv6</b>	Clears IP version 6 software-installed entries.
<b>destination</b> <i>ipv6-addr</i>	(Optional) Specifies a destination full IPv6 address or a subnet address. See the “Usage Guidelines” section for formatting guidelines.
<i>ipv6-prefix</i>	(Optional) IPv6 prefix; valid values are from 0 to 128.
<b>source</b> <i>ipv6-addr</i>	(Optional) Specifies a source full IPv6 address or a subnet address. See the “Usage Guidelines” section for formatting guidelines.
<b>flow</b> <b>tcp</b>	(Optional) Clears TCP flow information.
<b>flow</b> <b>udp</b>	(Optional) Clears UDP flow information.
<b>destination</b> <i>port-num</i>	(Optional) Specifies a destination port number.
<b>source</b> <i>port-num</i>	(Optional) Specifies a source port number.
<b>mpls</b>	Clears MPLS software-installed entries.
<b>top-label</b> <i>entry</i>	(Optional) Clears top-label entries; valid values are from 1 to 4294967295.
<b>ipx</b>	Clears IPX MLS entries.
<b>destination</b> <i>ipx-network</i>	(Optional) Specifies the destination IPX address. See the “Usage Guidelines” section for formatting guidelines.
<i>ipx-node</i>	(Optional) IPX node address. See the “Usage Guidelines” section for formatting guidelines.

<b>source</b> <i>ipx-network</i>	(Optional) Specifies the source IPX address. See the “Usage Guidelines” section for formatting guidelines.
<b>macs</b> <i>mac-addr</i>	(Optional) Specifies the source MAC addresses to consider when searching for entries to purge.
<b>macd</b> <i>mac-addr</i>	(Optional) Specifies the destination MAC addresses to consider when searching for entries to purge.
<b>interface</b> <i>interface-num</i>	(Optional) Clears entries that are associated with the specified VLAN or interface.
<b>all</b>	(Optional) Clears all entries.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC

**Command History**

Release	Modification
12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

When entering the IPX address syntax, use the following format:

- IPX network address—1..FFFFFFFE
- IPX node address—x.x.x where x is 0..FFFF
- IPX address—ipx\_net.ipx\_node (for example, 3.0034.1245.AB45, A43.0000.0000.0001)

Entering any combination of input parameters narrows the search of entries to be cleared. The **destination** or **source** *port-num* keyword and argument should be specified as one of the following: telnet, FTP, WWW, SMTP, X, or DNS.

Up to 16 routers can be included explicitly as MLS-RPs.

Use the following syntax to specify an IP subnet address:

- *ip-subnet-addr* or *ipv6-subnet-addr*—Short subnet address format. The trailing decimal number 00 in an IP or IPv6 address YY.YY.YY.00 specifies the boundary for an IP or IPv6 subnet address. For example, 172.22.36.00 indicates a 24-bit subnet address (subnet mask 172.22.36.00/255.255.255.0), and 173.24.00.00 indicates a 16-bit subnet address (subnet mask 173.24.00.00/255.255.0.0). However, this format can identify only a subnet address of 8, 16, or 24 bits.
- *ip-addr/subnet-mask* or *ipv6-addr/subnet-mask*—Long subnet address format. For example, 172.22.252.00/255.255.252.00 indicates a 22-bit subnet address. This format can specify a subnet address of any bit number. To provide more flexibility, the *ip-addr* or *ipv6-addr* is a full host address, such as 172.22.253.1/255.255.252.00.
- *ip-addr/maskbits* or *ipv6-addr/maskbits*—Simplified long subnet address format. The mask bits specify the number of bits of the network masks. For example, 172.22.252.00/22 indicates a 22-bit subnet address. The *ip-addr* or *ipv6-addr* is a full host address, such as 193.22.253.1/22, which has the same subnet address as the *ip-subnet-addr* or *ipv6-subnet-addr*.

If you do not use the **all** keyword, you must specify at least one of the other four keywords (**source**, **destination**, **flow**, or **interface**) and its arguments.

A 0 value for the **destination** or **source** *port-num* keyword and argument clears all entries. Unspecified options are treated as wildcards, and all entries are cleared.

### Examples

This example shows how to clear all the entries that are associated with a specific module (2) and that have a specific destination IP address (173.11.50.89):

```
Router# clear mls netflow ip destination 173.11.50.89 module 2
Router#
```

This example shows how to clear the IPv6 software-installed entries:

```
Router# clear mls netflow ipv6
Router#
```

This example shows how to clear the statistical information:

```
Router# clear mls netflow dynamic
Router#
```

### Related Commands

Command	Description
<a href="#">show mls netflow ip</a>	Displays information about the hardware NetFlow IP.
<a href="#">show mls netflow ipv6</a>	Displays information about the hardware NetFlow IPv6 configuration.

# clear mls qos

To clear the MLS aggregate-QoS statistics, use the **clear mls qos** command.

```
clear mls qos [{ip | ipx | mac | mpls | ipv6 | arp} [{interface interface-number} |
  {null interface-number} | {port-channel number} | {vlan vlan-id}]]
```

Syntax Description		
<b>ip</b>	(Optional)	Clears MLS IP aggregate-QoS statistics.
<b>ipx</b>	(Optional)	Clears MLS IPX aggregate-QoS statistics.
<b>mac</b>	(Optional)	Clears MLS MAC aggregate-QoS statistics.
<b>mpls</b>	(Optional)	Clears MLS MPLS aggregate-QoS statistics.
<b>ipv6</b>	(Optional)	Clears MLS IPv6 aggregate QoS statistics.
<b>arp</b>	(Optional)	Clears MLS ARP aggregate QoS statistics.
<i>interface</i>	(Optional)	Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , and <b>tengigabitethernet</b> . See the “Usage Guidelines” section for additional valid values.
<i>interface-number</i>	(Optional)	Module and port number; see the “Usage Guidelines” section for valid values.
<b>null</b> <i>interface-number</i>	(Optional)	Specifies the null interface; the valid value is <b>0</b> .
<b>port-channel</b> <i>number</i>	(Optional)	Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 256.
<b>vlan</b> <i>vlan-id</i>	(Optional)	Specifies the VLAN ID; valid values are from 1 to 4094.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines



### Note

Entering the **clear mls qos** command affects the policing token bucket counters and might allow traffic to be forwarded that would otherwise be policed.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

If you enter the **clear mls qos** command with no arguments, the global and per-interface aggregate QoS counters for all protocols are cleared.

If you do not enter an interface type, the protocol aggregate-QoS counters for all interfaces are cleared.

---

**Examples**

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

```
Router# clear mls qos
Router#
```

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

```
Router# clear mls qos ip
Router#
```

---

**Related Commands**

Command	Description
<a href="#">show mls qos</a>	Displays MLS QoS information.

# clear mls statistics

To reset the MLS statistics counters, use the **clear mls statistics** command.

**clear mls statistics** [*module num*]

<b>Syntax Description</b>	<b>module num</b> (Optional) Specifies the module number.
---------------------------	---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	This command replaces the <b>clear mls stats</b> command.
-------------------------	---

<b>Examples</b>	This example shows how to reset the MLS statistics counters for all modules:
-----------------	--

```
Router# clear mls statistics
Router#
```

This example shows how to reset the MLS statistics counters for a specific module:

```
Router# clear mls statistics module 5
Router#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show mls statistics</a>	Displays the MLS statistics for the IP, IPX, multicast, Layer 2 protocol, and QoS.

# clear mls stats

To clear the MLS statistics, use the **clear mls stats** command.

## clear mls stats

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

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to clear the MLS statistics for all modules:

```
Router# clear mls stats
Router#
```

Related Commands	Command	Description
	<a href="#">clear mls statistics</a>	Resets the MLS statistics counters.

# clear pagp

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

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

Syntax Description	
<i>group-number</i>	Channel group number; valid values are a maximum of 64 values from 1 to 256.
<b>counters</b>	Clears traffic filters.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

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

```
Router# clear pagp 324
Router#
```

This example shows how to clear the port-channel traffic filters:

```
Router# clear pagp counters
Router#
```

Related Commands	Command	Description
	<a href="#">show pagp</a>	Displays port-channel information.

# clear platform netint

To clear the interrupt-throttling counters for the platform, use the **clear platform netint** command.

## **clear platform netint**

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

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to clear the interrupt-throttling counters for the platform:

```
Router# clear platform netint
Router#
```

Related Commands	Command	Description
	<a href="#">show platform netint</a>	Displays the platform network-interrupt information.

# clear port-security

To delete configured secure MAC addresses and sticky MAC addresses from the MAC address table, use the **clear port-security** command.

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

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

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command is supported on negotiated trunks only.

If you enter the **clear port-security** command without adding any keywords or arguments, the switch removes all the secure MAC addresses and sticky MAC addresses from the MAC address table.

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

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

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

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

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

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

Related Commands	Command	Description
	<a href="#">show port-security</a>	Displays information about the port-security setting.
	<a href="#">switchport port-security mac-address</a>	Adds a MAC address to the list of secure MAC addresses.

# clear spanning-tree detected-protocol

To restart the protocol migration, use the **clear spanning-tree detected-protocol** command.

**clear spanning-tree detected-protocol** [**interface** *interface interface-num*]

<b>Syntax Description</b>	<b>interface</b>	(Optional) Specifies the interface type and number; possible valid values for type are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>port-channel</b> , and <b>vlan</b> . See the “Usage Guidelines” section for additional valid values.
	<b>interface</b> <i>interface</i>	
	<b>interface-num</b>	Module and port number; see the “Usage Guidelines” section for valid values for <b>port-channel</b> and <b>vlan</b> .

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

**Command Modes** EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** RSTP and MST have built-in compatibility mechanisms that allow them to interact properly with other versions of IEEE spanning tree or other regions. For example, a bridge running RSTP can send 802.1D BPDUs on one of its ports when it is connected to a legacy bridge. An MST bridge can detect that a port is at the boundary of a region when it receives a legacy BPDU or an MST BPDU that is associated with a different region. These mechanisms are not always able to revert to the most efficient mode. For example, an RSTP bridge that is designated for a legacy 802.1D stays in 802.1D mode even after the legacy bridge has been removed from the link. Similarly, an MST port assumes that it is a boundary port when the bridges to which it is connected have joined the same region. To force the MST port to renegotiate with the neighbors, enter the **clear spanning-tree detected-protocol** command.

The valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 2 to 13 and valid values for the port number are 1 to 48.

The number of valid values for **port-channel number** are a maximum of 64 values ranging from 1 to 256.

If you enter the **clear spanning-tree detected-protocol** command with no arguments, the command is applied to every port of the Catalyst 6500 series switch.

---

**Examples**

This example shows how to restart the protocol migration on a specific interface:

```
Router# clear spanning-tree detected-protocol fa1/1
Router#
```

---

**Related Commands**

Command	Description
<a href="#">show spanning-tree mst</a>	Displays information about the MST protocol.

---

# clear top counters interface report

To clear the TopN reports, use the **clear top counters interface report** command.

**clear top counters interface report** *number*

<b>Syntax Description</b>	<i>number</i> (Optional) Number of ports to be displayed; valid values are from 1 to 5000 physical ports.
---------------------------	---

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

**Command Modes** EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command is supported on Ethernet, Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet ports only. LAN ports on the OSMs are also supported.

The **clear top interface report** command clears all the completed reports. It does not clear the pending TopN reports. When you specify a report number, the TopN task is cleared regardless of its status.

**Examples** This example shows how to clear all TopN tasks:

```
Router# clear top counters interface report
04:00:06: %TOPN_COUNTERS-5-DELETED: TopN report 4 deleted by the console
04:00:06: %TOPN_COUNTERS-5-DELETED: TopN report 5 deleted by the console
04:00:06: %TOPN_COUNTERS-5-DELETED: TopN report 3 deleted by the console
04:00:06: %TOPN_COUNTERS-5-DELETED: TopN report 4 deleted by the console4/54/
Router#
```

This example shows the output if you attempt to clear a pending TopN task:

```
Router# clear top counters interface report 4
04:55:45: %TOPN_COUNTERS-5-KILLED: TopN report 4 killed by the sattili onvty0 (914016919)
Router#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">collect top counters interface</a>	Lists the TopN processes and specific TopN reports.
	<a href="#">show top counters interface report</a>	Displays TopN reports and 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**

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

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

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

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

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show vlan counters</a>	Displays the software-cached counter values.

# clock

To configure the port clocking mode for the 1000BASE-T transceivers, use the **clock** command. To return to the default settings, use the **no** form of this command.

**clock** { **auto** | **active** [**prefer**] | **passive** [**prefer**] }

**no clock**

Syntax Description	Parameter	Description
	<b>auto</b>	Enables the automatic clock configuration.
	<b>active</b>	Enables the active operation.
	<b>prefer</b>	(Optional) Negotiates the specified mode with the far end of the link.
	<b>passive</b>	Enables the passive operation.

**Defaults** **auto**

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

This command is supported on the 1000BASE-T transceivers only.

If the clock mode of the near end of a link does not match the clock mode of the far end, the line protocol does not come up.

The active and passive clock status is determined during autonegotiation before the transmission link is established.

The **clock** command supports the following configurations:

- **auto**—Autonegotiates with the far end of the link but gives preference to the active-clock switch.
- **active**—Uses a local clock to determine transmitter-operation timing.
- **passive**—Recovers the clock from the received signal and uses the recovered clock to determine transmitter-operation timing.
- **active prefer**—Autonegotiates with the far end of the link but gives preference to the active-clock switch.
- **passive prefer**—Autonegotiates with the far end of the link but gives preference to the passive-clock switch.

Enter the **show running-config interface** command to display the current clock mode.

Enter the **show interfaces** command to display the clock mode that is negotiated by the firmware.

---

**Examples**

This example shows how to enable the active-clock operation:

```
Router(config-if)# clock active  
Router(config-if)#
```

---

**Related Commands**

Command	Description
<a href="#">show interfaces</a>	Displays the traffic that is seen by a specific interface.
<a href="#">show running-config interface</a>	Displays the status and configuration of the module or Layer 2 VLAN.

# collect top counters interface

To list the TopN processes and specific TopN reports, use the **collect top counters interface** command.

**collect top** [*number*] **counters interface** *interface-type* [**interval** *seconds*] [**sort-by** *sort-by-value*]

## Syntax Description

<i>number</i>	(Optional) Number of ports to be displayed; valid values are from 1 to 5000 physical ports.
<i>interface-type</i>	Type of ports to be used in the TopN request; valid values are <b>all</b> , <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>layer-2 vlan-num</b> , and <b>layer-3</b> .
<b>interval</b> <i>seconds</i>	(Optional) Specifies the interval over which the statistics is gathered; valid values are from 0 to 999 seconds.
<b>sort-by</b> <i>sort-by-value</i>	(Optional) Specifies the port statistic to generate the report on; valid values are as follows: <ul style="list-style-type: none"> <li>• <b>broadcast</b>—Sorts the report based on the receive and transmit broadcast packets.</li> <li>• <b>bytes</b>—Sorts the report based on the receive and transmit bytes.</li> <li>• <b>errors</b>—Sorts the report based on the receive errors.</li> <li>• <b>multicast</b>—Sorts the report based on the receive and transmit multicast packets.</li> <li>• <b>overflow</b>—Sorts the report based on the transmit overflow errors.</li> <li>• <b>packets</b>—Sorts the report based on the receive and transmit packets.</li> <li>• <b>utilization</b>—Sorts the report based on the port utilization.</li> </ul>

## Defaults

The defaults are as follows:

- *number* is **20** physical ports.
- *sort-by-value* is **util**.
- *seconds* is **30** seconds.
- *interface-type* is **all**.

## Command Modes

EXEC

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

This command is supported on Ethernet, Fast Ethernet, Gigabit Ethernet and 10-Gigabit Ethernet ports only. LAN ports on the OSMs are also supported.

If you specify an interval of **0** seconds, the TopN report is generated based on the absolute counters value. You cannot specify the **interval seconds** keyword and argument when the sorting criteria is **utilization** because utilization can only be computed over an interval.

When you specify the **layer-2 vlan-num**, valid values are from 1 to 4094 and indicates the number of the Layer 2 interface.

Only a TopN task with a done status is allowed to display the report. If you try to view a report that is incomplete (pending), an appropriate message is displayed.

The TopN utility collects the following port utilization data for each physical port over the *seconds* interval:

- Total number of in and out bytes.
- Total number of in and out packets.
- Total number of in and out broadcast packets.
- Total number of in and out multicast packets.
- Total number of in errors (Ethernet ports such as CRC, undersize packets (+Runt), oversize packets, fragmentation, and jabber).
- Total number of buffer-overflow errors including outlost packets; for example, these errors include transmit errors that are due to these buffer full and Ethernet ports: dmaTxOverflow and dmaTxFull.

After the collection of information, the ports are sorted according to the *sort-by-value* argument, and the top *number* of ports are displayed.

When the TopN reports are ready, a syslog message is displayed that the TopN reports are available. You can use the **show top interface report** command to view the reports. You can display the TopN reports multiple times until you enter the **clear top interface report** command to clear the reports.

Use the **clear top interface report** command to clear the reports.

**Examples**

This example shows how to sort the TopN report based on the receive and transmit broadcast packets:

```
Router# collect top 40 counters interface all sort-by broadcast
Router#
```

This example shows how to sort the TopN report based on the receive and transmit broadcast packets and specify the TopN sampling interval:

```
Router# collect top 40 counters interface all sort-by broadcast interval 500
Router#
```

**Related Commands**

Command	Description
<a href="#">clear top counters interface report</a>	Clears the TopN reports.
<a href="#">show top counters interface report</a>	Displays TopN reports and information.

# 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** No control plane service policies are defined.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines



### 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 aggregate 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:

```
Router(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
! Allow 40141415 trusted host traffic1
Router(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
! Rate limit all other Telnet traffic1
Router(config)# access-list 140 permit tcp any any eq telnet
! Define class-map "telnet-class1"
Router(config)# class-map telnet-class
Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map control-plane
Router(config-pmap)# class telnet-class
```

```

Router(config-pmap-c)# police 80000 conform transmit exceed drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
! Define aggregate control plane service for the active Route Processor1
Router(config)# control-plane
Router(config-cp)# service-policy input control-plane-policy
Router(config-cp)# exit

```

**Related Commands**

Command	Description
<a href="#">class (policy-map)</a>	Specifies the name of the class that has a policy that you want to create or change or to specify the default class (commonly known as the class-default class) before you configure its policy.
<a href="#">class-map</a>	Accesses the QoS class-map configuration mode to configure QoS class maps.
<a href="#">drop</a>	Configures a traffic class to discard packets belonging to a specific class.
<a href="#">match access-group</a>	Configures the match criteria for a class map on the basis of the specified ACL.
<a href="#">policy-map</a>	Accesses QoS policy-map configuration mode to configure the QoS policy map.
<a href="#">service-policy (control-plane)</a>	Attaches a policy map to a control plane for aggregate control plane services.
<a href="#">show policy-map control-plane</a>	Displays the configuration either of a class or of all classes for the policy map of a control plane.

## copy /noverify

To disable the automatic image verification for the current copy operation, use the **copy /noverify** command.

**copy /noverify** *source-url destination-url*

### Syntax Description

<i>source-url</i>	Location URL or alias of the source file or directory to be copied; see the “Usage Guidelines” section for additional information.
<i>destination-url</i>	Destination URL or alias of the copied file or directory; see the “Usage Guidelines” section for additional information.

### Defaults

Verification is done automatically after completion of a copy operation.

### Command Modes

EXEC

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

The exact format of the source and destination URLs varies according to the file or directory location. You may enter either an alias keyword for a particular file or an alias keyword for a file system type (not a file within a type).



#### Timesaver

Aliases are used to cut down on the amount of typing that you need to perform. For example, it is easier to type **copy run start** (the abbreviated form of the **copy running-config startup-config** command) than it is to type **copy system:r nvram:s** (the abbreviated form of the **copy system:running-config nvram:startup-config** command). These aliases allow you to continue using some of the common commands that are used in previous versions of Cisco IOS software.

[Table 2-3](#) shows two keyword shortcuts to URLs.

**Table 2-3 Common Keyword Aliases to URLs**

Keyword	Source or Destination
<b>running-config</b>	(Optional) Specifies the alias for the <b>system:running-config</b> URL. This keyword does not work in the <b>more</b> and <b>show file</b> command syntaxes.
<b>startup-config</b>	(Optional) Specifies the alias for the <b>nvram:startup-config</b> URL. The <b>nvram:startup-config</b> keyword represents the configuration file that is used during initialization (startup). This file is contained in NVRAM. This keyword does not work in <b>more</b> and <b>show file</b> EXEC command syntaxes.

Table 2-4 through Table 2-6 list aliases by file system type. If you do not specify an alias, the system looks for a file in the current directory.

Table 2-4 lists the URL prefix aliases for special (opaque) file systems, Table 2-5 lists the URL prefix aliases for network file systems, and Table 2-6 lists the URL prefix aliases for local writable storage file systems.

**Table 2-4 URL Prefix Aliases for Special File Systems**

Alias	Source or Destination
<b>flh:</b>	Source URL for flash load helper log files.
<b>nvr:</b>	Router NVRAM. You can copy the startup configuration into or from NVRAM. You can also display the size of a private configuration file.
<b>null:</b>	Null destination for copies or files. You can copy a remote file to null to determine its size.
<b>system:</b>	Source or destination URL for system memory, which includes the running configuration.
<b>xmodem:</b>	Source destination for the file from a network device that uses the Xmodem protocol.
<b>ymodem:</b>	Source destination for the file from a network device that uses the Ymodem protocol.

**Table 2-5 URL Prefix Aliases for Network File Systems**

Alias	Source or Destination
<b>ftp:</b>	Source or destination URL for an FTP network server. The syntax for this alias is as follows: <b>ftp:[[/username[:password]@]location]/directory]/filename.</b>
<b>rcp:</b>	Source or destination URL for an rcp network server. The syntax for this alias is as follows: <b>rcp:[[/username@]location]/directory]/filename.</b>
<b>tftp:</b>	Source or destination URL for a TFTP network server. The syntax for this alias is <b>tftp:[/location]/directory]/filename.</b>

**Table 2-6 URL Prefix Aliases for Local Writable Storage File Systems**

Alias	Source or Destination
<b>bootflash:</b>	Source or destination URL for boot flash memory.
<b>disk0: and disk1:</b>	Source or destination URL of rotating media.
<b>flash:</b>	Source or destination URL for flash memory. This alias is available on all platforms.  For platforms that lack a flash device, note that <b>flash:</b> is aliased to <b>slot0:</b> , allowing you to refer to the main flash memory storage area on all platforms.



# define interface-range

To create an interface-range macro, use the **define interface-range** command.

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

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

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

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The macro name is a 32-character maximum character string.  
A macro can contain up to five ranges. An interface range cannot span slots. When entering the *interface-range*, these formats can be used:

- *card-type* {*slot*}/{*first-interface*} - {*last-interface*}
- *card-type* {*slot*}/{*first-interface*} - {*last-interface*}

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

- **ethernet**
- **fastethernet**
- **gigabitethernet**
- **loopback**
- **tengigabitethernet**
- **tunnel**
- **vlan** *vlan-id* (valid values are from 1 to 4094)
- **port-channel** *interface-number* (valid values are from 1 to 256)

## ■ define interface-range

---

**Examples**

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

```
Router(config)# define interface-range macro1 ethernet 1/2 - 5, fastethernet 5/5 - 10
Router(config)#
```

---

**Related Commands**

Command	Description
<a href="#">interface range</a>	Executes a command on multiple ports at the same time.

# diagnostic bootup level

To set the bootup diagnostic level, use the **diagnostic bootup level** command. To skip all diagnostic tests, use the **no** form of this command.

**diagnostic bootup level { minimal | complete }**

**default diagnostic bootup level**

**no diagnostic bootup level**

Syntax Description	minimal	complete	default
	Specifies minimal diagnostics; see the “Usage Guidelines” section for additional information.	Specifies complete diagnostics; see the “Usage Guidelines” section for additional information.	Returns to the default setting.

**Defaults** minimal

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Setting the diagnostic level determines the level of testing that occurs when the system or module is reset. The two levels are as follows:

- Complete—Runs all tests.
- Minimal—Runs only EARL tests for the supervisor engine and loopback tests for all ports in the system.



**Note** Although the default is **minimal**, you can set the diagnostic level to **complete** for troubleshooting hardware problems.

In certain circumstances, you might want to skip the bootup online diagnostics completely. For example, you might skip the bootup online diagnostics to verify that a port is as bad as online diagnostics reports. To skip online diagnostic testing completely, enter the **no diagnostic bootup level** command.

For information on the diagnostic test types, see the [show diagnostic](#) command.

The new level takes effect at the next reload or the next time that an online insertion and removal is performed.

---

### Examples

This example shows how to set the bootup diagnostic level:

```
Router(config)# diagnostic bootup level complete
Router(config)#
```

---

### Related Commands

Command	Description
<a href="#">show diagnostic bootup level</a>	Displays the coverage level for the configured boot-up diagnostics.

# diagnostic cns

To configure the CNS diagnostics, use the **diagnostic cns** command. To disable sending diagnostic results to the CNS event bus, use the **no** form of this command.

**diagnostic cns** {**publish** | **subscribe**} [*subject*]

**default diagnostic cns** {**publish** | **subscribe**}

**no diagnostic cns** {**publish** | **subscribe**} [*subject*]

Syntax Description		
	<b>publish</b>	Sends diagnostic results to a remote network application to make decisions and take corrective actions that are based on the diagnostic results.
	<b>subscribe</b>	Receives messages from remote network applications to perform diagnostic tests or retrieve diagnostic results.
	<i>subject</i>	(Optional) Event subject name.
	<b>default</b>	Sets the default.

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

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The online diagnostics receive events by subscribing to an event *subject* name. The *subject* is the event that you subscribe (receive) or publish (generate) through the CNS bus.

The **diagnostic cns publish** command sends diagnostic results to a remote network application to make decisions and take corrective actions that are based on the diagnostic results.

The **diagnostic cns subscribe** command receives messages from remote network applications to perform diagnostic tests or retrieve diagnostic results.

**Examples** This example shows how to enable the publishing of diagnostic results:

```
Router(config)# diagnostic cns publish
Router(config)#
```

This example shows how to receive messages from remote network applications to perform diagnostic tests or retrieve diagnostic results:

```
Router(config)# diagnostic cns subscribe
Router(config)#
```

This example shows how to set the default to **publish**:

```
Router(config)# default diagnostic cns publish
Router(config)#
```

---

**Related Commands**

Command	Description
<a href="#">show diagnostic cns</a>	Displays the information about the CNS subject.

# diagnostic event-log size

To modify the diagnostic event-log size dynamically, use the **diagnostic event-log size** command. To return to the default settings, use the **no** form of this command.

**diagnostic event-log size** *size*

**default diagnostic event-log size**

**no diagnostic event-log size**

Syntax Description	
<i>size</i>	Diagnostic event-log size; valid values are from 1 to 10000 entries.
<b>default</b>	Returns to the default setting.

**Defaults** The *size* is **500** entries.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The events are dynamically allocated and stored in a circular queue.  
You can enter either the **default diagnostic event-log size** command or the **no diagnostic event-log size** command to return to the default settings.

**Examples** This example shows how to set the diagnostic event-log size:

```
Router(config)# diagnostic event-log size 600
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show diagnostic events</a>	Displays the event log for the diagnostic events.

# diagnostic monitor

To configure the health-monitoring diagnostic testing, use the **diagnostic monitor** command. To disable testing, use the **no** form of this command.

```
diagnostic monitor interval {module num} test {test-id | test-id-range | all} [hour hh] [min mm]
[second ss] [millisec ms] [day day]
```

```
diagnostic monitor syslog
```

```
diagnostic monitor {module num} test {test-id | test-id-range | all}
```

```
no diagnostic monitor {interval | syslog}
```

Syntax Description		
<b>interval</b>		Sets the interval between testing.
<b>module num</b>		Specifies the module number.
<b>test</b>		Specifies a test to run.
<i>test-id</i>		Identification number for the test to be run; see the “Usage Guidelines” section for additional information.
<i>test-id-range</i>		Range of identification numbers for tests to be run; see the “Usage Guidelines” section for additional information.
<b>all</b>		Runs all the diagnostic tests.
<b>hour hh</b>		(Optional) Specifies the number of hours between tests; see the “Usage Guidelines” section for formatting guidelines.
<b>min mm</b>		(Optional) Specifies the number of minutes between tests; see the “Usage Guidelines” section for formatting guidelines.
<b>second ss</b>		(Optional) Specifies the number of seconds between tests; see the “Usage Guidelines” section for formatting guidelines.
<b>millisec ms</b>		(Optional) Specifies the number of milliseconds between tests; see the “Usage Guidelines” section for formatting guidelines.
<b>day day</b>		(Optional) Specifies the number of days between tests; see the “Usage Guidelines” section for formatting guidelines.
<b>syslog</b>		Enables the generation of a syslog message when a health-monitoring test fails.

## Defaults

The defaults are as follows:

- Depending on the test run, monitoring may be enabled or disabled.
- Depending on the test run, the default monitoring interval varies.
- **syslog** is enabled.

## Command Modes

Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

Use these guidelines when scheduling testing:

- *test-id*—Enter the **show diagnostic content** command to display the test ID list.
- *test-id-range*—Enter the **show diagnostic content** command to display the test ID list. Enter the range as integers separated by a comma and a hyphen (for example, 1,3-6 specifies test IDs 1, 3, 4, 5, and 6).
- *hh*—Enter the hours from 1 to 24.
- *mm*—Enter the minutes from 1 to 60.
- *day*—Enter the day of the week as a number from 1 to 7 (**1** is Sunday).
- *ss*—Enter the seconds from 1 to 60.
- *ms*—Enter the milliseconds from 1 to 1000.

Enter the **[no] diagnostic monitor test {test-id | test-id-range | all}** command to enable or disable the specified health monitoring test.

When entering the **diagnostic monitor {module num} test {test-id | test-id-range | all}** command, observe the following:

- Required
  - Isolate network traffic by disabling all connected ports and do not pump test packets during the test.
  - Remove all modules for testing FIB TCAM and SSRAM memory on the PFC of the supervisor engine.
  - Reset the system or the test module before putting the system back into the normal operating mode.
- Recommended
  - Turn off all background health-monitoring tests on the supervisor engine and the modules using the **no diagnostic monitor {module num} test {test-id | test-id-range | all}** command.

The FIB TCAM test for central PFC3B (on the supervisor engine) takes approximately 4 hours and 30 minutes.

The FIB TCAM test takes approximately 16 hours.

### Examples

This example shows how to run the specified test every 3 days, 10 hours, and 2 minutes:

```
Router(config)# diagnostic monitor interval module 1 test 1 day 3 hours 10 min 2
Router(config)#
```

This example shows how to enable the generation of a syslog message when any health-monitoring test fails:

```
Router(config)# diagnostic monitor syslog
Router(config)#
```

### Related Commands

■ diagnostic monitor

Command	Description
<b>show diagnostic content</b>	Displays test information including test ID, test attributes, and supported coverage test levels for each test and for all modules.

# diagnostic ondemand

To configure the ondemand diagnostics, use the **diagnostic ondemand** command.

```
diagnostic ondemand { iteration iteration-count } | { action-on-error { continue | stop }
[error-count] }
```

Syntax Description	iteration <i>iteration-count</i>	Sets the number of times that the same test will be rerun when the command is issued.
	<b>action-on-error</b>	Sets the execution action when an error is detected.
	<b>continue</b>	Continues testing when a test failure is detected.
	<b>stop</b>	Stops testing when a test failure is detected.
	<i>error-count</i>	(Optional) Number of errors that are allowed before stopping; used with the <b>continue</b> option.

## Defaults

The default settings are as follows:

- *iteration-count* is **1**.
- **action-on-error** is **continue**.
- *error-count* is **0**.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

Entering **0** for the *error-count* sets the number of errors that are allowed to unlimited.

## Examples

This example shows how to set the on-demand testing iteration count:

```
Router# diagnostic ondemand iteration 4
Router#
```

This example shows how to set the execution action when an error is detected:

```
Router# diagnostic ondemand action-on-error continue 2
Router#
```

## Related Commands

Command	Description
<a href="#">show diagnostic ondemand</a>	Displays the settings for the on-demand diagnostics.

# diagnostic schedule test

To set the scheduling of test-based diagnostic testing for a specific module or schedule a supervisor engine switchover, use the **diagnostic schedule test** command. To remove the scheduling, use the **no** form of this command.

**diagnostic schedule** { **module** { *num* | *active-sup-slot* } } **test** { *test-id* | *test-id-range* | **all** } [**port** { *num* | *num-range* | **all** } ] { **on** *mm dd yyyy hh:mm* } | { **daily** *hh:mm* } | { **weekly** *day-of-week hh:mm* }

**no diagnostic schedule test**

Syntax Description		
<b>module</b> <i>num</i>		Specifies the module number.
<b>module</b> <i>active-sup-slot</i>		Specifies the slot number of the active supervisor engine.
<i>test-id</i>		Identification number for the test to be run; see the “Usage Guidelines” section for additional information.
<i>test-id-range</i>		Range of identification numbers for tests to be run; see the “Usage Guidelines” section for additional information.
<b>all</b>		Runs all diagnostic tests.
<b>port</b>		(Optional) Specifies the port to schedule testing.
<i>num</i>		Port number.
<i>num-range</i>		Range of port numbers, separated by a hyphen.
<b>all</b>		Specifies all ports.
<b>on</b> <i>mm dd yyyy hh:mm</i>		Specifies the scheduling of a test-based diagnostic task; see the “Usage Guidelines” section for formatting guidelines.
<b>daily</b> <i>hh:mm</i>		Specifies the daily scheduling of a test-based diagnostic task; see the “Usage Guidelines” section for formatting guidelines.
<b>weekly</b> <i>day-of-week hh:mm</i>		Specifies the weekly scheduling of a test-based diagnostic task; see the “Usage Guidelines” section for formatting guidelines.

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

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

Use these guidelines when scheduling testing:

- *test-id*—Enter the **show diagnostic content** command to display the test ID list.
- *test-id-range*—Enter the **show diagnostic content** command to display the test ID list. Enter the range as integers separated by a comma and a hyphen (for example, 1,3-6 specifies test IDs 1, 3, 4, 5, and 6).
- *num-range*—Enter the range as integers separated by a comma and a hyphen (for example, you can enter 1,3-6 to specify ports 1, 3, 4, 5, and 6).
- *mm*—Spell out the month such as january, february ... december (either uppercase or lowercase characters).
- *dd*—Enter the day as a 2-digit number.
- *yyyy*—Enter the year as a 4-digit number.
- *hh:mm*—Enter the time as a 2-digit number (for a 24-hour clock) for hours:minutes; the colon (:) is required.
- *day-of-week*—Spell out the day of the week, such as monday, tuesday... sunday (either uppercase or lowercase characters).
- **port {num | num-range | all}**—Is not supported when specifying a scheduled switchover.

Enter the **show diagnostic content** command to display the test ID list.

You can use the **diagnostic schedule module active-sup-slot test test-id** command to schedule a switchover from the active supervisor engine to the standby supervisor engine.

Enter the **show diagnostic content active-sup-slot** command to display the test ID list and look for the test ID in the ScheduleSwitchover field.

You can specify a periodic switchover (daily or weekly) or a single switchover occurrence at a specific time using these commands:

- **diagnostic schedule module active-sup-slot test test-id on mm dd yyyy hh:mm**
- **diagnostic schedule module active-sup-slot test test-id daily hh:mm**
- **diagnostic schedule module active-sup-slot test test-id weekly day-of-week hh:mm**

**Note**

To avoid system downtime if the standby supervisor engine cannot switch over the system, we recommend that you schedule a switchover from the standby supervisor engine to the active supervisor engine 10 minutes after the switchover occurs. See the “Examples” section for additional information.

**Examples**

This example shows how to schedule the diagnostic testing on a specific date and time for a specific module and port:

```
Router(config)# diagnostic schedule module 1 test 1,2,5-9 port 3 on january 3 2003 23:32
Router(config)#
```

This example shows how to schedule the diagnostic testing to occur daily at a certain time for a specific port and module:

```
Router(config)# diagnostic schedule module 1 test 1,2,5-9 port 3 daily 12:34
Router(config)#
```

This example shows how to schedule the diagnostic testing to occur weekly on a certain day for a specific port and module:

```
Router(config)# diagnostic schedule module 1 test 1,2,5-9 port 3 weekly friday 09:23
Router(config)#
```

This example shows how to schedule a switchover for the active supervisor engine every Friday at 10:00 pm, and switch the standby supervisor engine back to the active supervisor engine 10 minutes after the switchover occurs. For this example, these conditions apply:

- *test-id* is 32.
- The active supervisor engine is in slot 5.
- The standby supervisor engine is in slot 6.

#### Related Commands

Command	Description
<a href="#">show diagnostic content</a>	Displays test information including test ID, test attributes, and supported coverage test levels for each test and for all modules.
<a href="#">show diagnostic schedule</a>	Displays the current scheduled diagnostic tasks.

# diagnostic start

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

**diagnostic start** { **module** *num* } **test** { *test-id* | *test-id-range* | **minimal** | **complete** | **basic** | **per-port** | **non-disruptive** | **all** } [**port** { *num* | *port#-range* | **all** }]

Syntax Description		
<b>module</b> <i>num</i>		Specifies the module number.
<b>test</b>		Specifies a test to run.
<i>test-id</i>		Identification number for the test to be run; see the “Usage Guidelines” section for additional information.
<i>test-id-range</i>		Range of identification numbers for tests to be run; see the “Usage Guidelines” section for additional information.
<b>minimal</b>		Runs minimal bootup diagnostic tests.
<b>complete</b>		Runs complete bootup diagnostic tests.
<b>basic</b>		Runs basic on-demand diagnostic tests.
<b>per-port</b>		Runs per-port level tests.
<b>non-disruptive</b>		Runs the nondisruptive health-monitoring tests.
<b>all</b>		Runs all diagnostic tests.
<b>port</b> <i>num</i>		(Optional) Specifies the interface port number.
<b>port</b> <i>port#-range</i>		Specifies the interface port number range; see the “Usage Guidelines” section for additional information.
<b>port all</b>		Specifies all ports.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines



**Note** We recommend that before you enable any online diagnostics tests that you enable the logging console/monitor to see all warning messages.



**Note** We recommend that when you are running disruptive tests that you only run the tests when connected through console. When disruptive tests are complete a warning message on the console recommends that that you reload the system to return to normal operation. Note: Strictly follow this warning.

**Note**

While this test is running, all ports are shut down as a stress test is being performed with looping ports internally and external traffic might skew the test results. The entire switch must be rebooted to bring the switch to normal operation. When you issue the command to reload the switch, the system will ask you if the configuration should be saved. Note: Do not save the configuration.

**Note**

If you are running the tests on a module that is not the supervisor engine, after the test is initiated and complete, you must reset the module.

**Note**

Do not enter the **diagnostic start module *x* test all** command on systems that are configured with a DFC3A because this command causes the TCAM test to fail.

Enter the **show diagnostic content** command to display the test ID list.

Enter the *test-id-range* or *port#-range* as integers separated by a comma and a hyphen (for example, 1,3-6 specifies test IDs 1, 3, 4, 5, and 6).

Use the **diagnostic stop** command to stop the testing process.

**Examples**

This example shows how to run the specified diagnostic test at the specified slot:

```
Router# diagnostic start module 1 test 5
Module 4:Running test(s) 5 may disrupt normal system operation
Do you want to run disruptive tests? [no]yes
00:48:44:Running OnDemand Diagnostics [Iteration #4] 111
00:48:44:%DIAG-SP-6-TEST_RUNNING:Module 4:Running TestNewLearn{ID=5} 111
00:48:44:%DIAG-SP-6-TEST_OK:Module 4:TestNewLearn{ID=5} has completed successfully
00:48:44:Running OnDemand Diagnostics [Iteration #5] 111
00:48:44:%DIAG-SP-6-TEST_RUNNING:Module 4:Running TestNewLearn{ID=5} 111
00:48:44:%DIAG-SP-6-TEST_OK:Module 4:TestNewLearn{ID=5} has completed successfully
Router#
```

**Related Commands**

Command	Description
<b>diagnostic stop</b>	Stops the testing process.
<b>show diagnostic</b>	Displays the test results of the online diagnostics and lists the supported test suites.

# diagnostic stop

To stop the testing process, use the **diagnostic stop** command.

**diagnostic stop** {**module** *num*}

<b>Syntax Description</b>	<b>module</b> <i>num</i> Module number.
---------------------------	---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	Use the <b>diagnostic start</b> command to start the testing process.
-------------------------	---

<b>Examples</b>	This example shows how to stop the diagnostic test process:
-----------------	---

```
Router# diagnostic stop module 3
Router#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>diagnostic start</b>	Runs the testing process.
	<b>show diagnostic</b>	Displays the test results of the online diagnostics and lists the supported test suites.

# disconnect qdm

To disconnect a QDM session, use the **disconnect qdm** command.

**disconnect qdm** [{**client** *client-id*}]

<b>Syntax Description</b>	<b>client</b> <i>client-id</i> (Optional) Specifies a client to disconnect.
---------------------------	---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	<p>QDM is not supported on OSM interfaces.</p> <p>If you enter the <b>disconnect qdm</b> command without any arguments, all QDM sessions are disconnected. You can obtain the <i>client-id</i> by entering the <b>show qdm status</b> command.</p>
-------------------------	--

<b>Examples</b>	This example shows how to disconnect a QDM session:
-----------------	---

```
Router# disconnect qdm client 1
Router#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show qdm status</b>	Displays information about the status for the currently active QDM clients who are connected to the Catalyst 6500 series switch.

# do

To execute the EXEC-level commands from global configuration mode or other configuration modes or submodes, use the **do** command.

**do** *command*

## Syntax Description

<i>command</i>	EXEC-level command to be executed.
----------------	------------------------------------

## Defaults

This command has no default settings.

## Command Modes

Global configuration or any other configuration mode or submode from which you are executing the EXEC-level command.

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines



### Caution

Do not enter the **do** command in EXEC mode. Interruption of service may occur.

You cannot use the **do** command to execute the **configure terminal** command because entering the **configure terminal** command changes the mode to configuration mode.

You cannot use the **do** command to execute the **copy** or **write** command in the global configuration or any other configuration mode or submode.

## Examples

This example shows how to execute the EXEC-level **show interfaces** command from within global configuration mode:

```
Router(config)# do show interfaces serial 3/0

Serial3/0 is up, line protocol is up
  Hardware is M8T-RS535
  MTU 4500 bytes, BW 4544 Kbit, DL\ 50000 usec, rely 555/555, load 4/555
  Encapsulation HDLC, loopback not set, keepalive set (40 sec)
  Last input never, output 4d47h, output hang never
  Last clearing of "show interface" counters never
  1
  1
  1
Router(config)#
```

## dot1x default

To reset the configurable 802.1X parameters to the default settings, use the **dot1x default** command.

### **dot1x default**

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

### Defaults

The default values are as follows:

- The per-interface 802.1X protocol enable state is disabled (force-authorized).
- The number of seconds between reauthentication attempts is 3600 seconds.
- The quiet period is 60 seconds.
- The retransmission time is 30 seconds.
- The maximum retransmission number is 2 times.
- The multiple host support is disabled.
- The client timeout period is 30 seconds.
- The authentication server timeout period is 30 seconds.

**Command Modes** Interface configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Examples

This example shows how to reset the configurable 802.1X parameters to the default values:

```
Router(config-if)# dot1x default
Setting the Default Configuration for Dot4x on this interface

Router(config-if)#
```

### Related Commands

Command	Description
<a href="#">show dot1x</a>	Displays 802.1X information.

## dot1x max-req

To set the number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process, use the **dot1x max-req** command. To return to the default settings, use the **no** form of this command.

**dot1x max-req** *count*

**no dot1x max-req**

<b>Syntax Description</b>	<i>count</i>	Number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process; valid values are from 1 to 10.
---------------------------	--------------	--

<b>Defaults</b>	The <i>count</i> is <b>2</b> .
-----------------	--------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	You should change the default value only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.
-------------------------	--

<b>Examples</b>	This example shows how to set 5 as the number of times that the switch sends an EAP-request/identity request before restarting the authentication process:
-----------------	--

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show dot1x</a>	Displays 802.1X information.

# dot1x multi-hosts

To allow multiple hosts (clients) on an 802.1X-authorized port, use the **dot1x multi-hosts** command. To disallow multiple hosts, use the **no** form of this command.

**dot1x multi-hosts**

**no dot1x multi-hosts**

---

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

---

**Defaults** Disabled

---

**Command Modes** Interface configuration

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Usage Guidelines** Before entering this command, ensure that the **dot1x port-control** command is set to **auto** for the specified interface.

---

**Examples** This example shows how to allow multiple hosts:

```
Router(config-if)# dot1x multi-hosts
Router(config-if)#
```

This example shows how to disallow multiple hosts:

```
Router(config-if)# no dot1x multi-hosts
Router(config-if)#
```

---

Related Commands	Command	Description
	<b>dot1x port-control</b>	Sets the port control value.
	<b>show dot1x</b>	Displays 802.1X information.

---

# dot1x port-control

To set the port control value, use the **dot1x port-control** command. To return to the default settings, use the **no** form of this command.

**dot1x port-control** *value*

**no dot1x port-control**

<b>Syntax Description</b>	<i>value</i>	Port-control value; valid values are <b>auto</b> , <b>force-authorized</b> , and <b>force-unauthorized</b> ; see the “Usage Guidelines” section for more information.
---------------------------	--------------	---

<b>Defaults</b>	<b>force-authorized</b>
-----------------	-------------------------

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

<b>Command History</b>	<table border="1"> <thead> <tr> <th style="border: none;">Release</th> <th style="border: none;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border: none;">12.2(18)ZY</td> <td style="border: none;">Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)ZY	Support for this command was introduced.
Release	Modification				
12.2(18)ZY	Support for this command was introduced.				

<b>Usage Guidelines</b>	<p>The port-control <i>value</i> definitions are as follows:</p> <ul style="list-style-type: none"> <li>• <b>force-authorized</b>—Disables 802.1X port-based authentication 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.</li> <li>• <b>force-unauthorized</b>—Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. Authentication services are not provided to the client through the interface.</li> <li>• <b>auto</b>—Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up or when an EAPOL-start frame is received. The system requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client attempting to access the network is uniquely identified by the system by using the client’s MAC address.</li> </ul>
-------------------------	--

To check the port-control configuration, enter the **show dot1x** command and check the Status column in the 802.1X Port Summary section. An *enabled* status means that the port-control value is set either to **auto** or to **force-unauthorized**.

---

**Examples**

This example shows how to set the port control to auto:

```
Router(config-if)# dot1x port-control auto
Router(config-if)#
```

---

**Related Commands**

Command	Description
<a href="#">show dot1x</a>	Displays 802.1X information.

---

# dot1x reauthentication

To enable periodic reauthentication of the client, use the **dot1x reauthentication** command. To return to the default settings, use the **no** form of this command.

**dot1x reauthentication**

**no dot1x reauthentication**

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

**Defaults** Disabled

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Reauthentication does not disturb the status of an already authorized port.

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

```
Router(config-if)# dot1x reauthentication
Router(config-if)#
```

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

```
Router(config-if)# no dot1x reauthentication
Router(config-if)#
```

Related Commands	Command	Description
	<a href="#">dot1x timeout</a>	Sets the reauthentication timer.
	<a href="#">show dot1x</a>	Displays 802.1X information.

# dot1x system-auth-control

To enable 802.1X globally, use the **dot1x system-auth-control** command. To disable 802.1X globally, 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** Disabled

---

**Command Modes** Global configuration

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Usage Guidelines** You must enable AAA and specify the authentication method list before enabling 802.1X. A method list describes the sequence and authentication methods to be queried to authenticate a user.

---

**Examples** This example shows how to enable 802.1X globally:

```
Router(config)# dot1x system-auth-control
Router(config)#
```

This example shows how to disable 802.1X globally:

```
Router(config)# no dot1x system-auth-control
Router(config)#
```

---

Related Commands	Command	Description
	<b>aaa authentication dot1x</b>	Specifies one or more AAA methods for use on interfaces running IEEE 802.1X.
	<b>aaa new-model</b>	Enables the AAA access-control model.
	<b>show dot1x</b>	Displays 802.1X information.

---

# dot1x timeout

To set the reauthentication timer, use the **dot1x timeout** command. To return to the default settings, use the **no** form of this command.

```
dot1x timeout {{ reauth-period seconds } | { quiet-period seconds } | { tx-period seconds } |
{ supp-timeout seconds } | { server-timeout seconds } }
```

```
no dot1x timeout { reauth-period | quiet-period | tx-period | supp-timeout | server-timeout }
```

## Syntax Description

<b>reauth-period</b> <i>seconds</i>	Specifies the number of seconds between reauthentication attempts; valid values are from 1 to 65535. See the “Usage Guidelines” section for additional information.
<b>quiet-period</b> <i>seconds</i>	Specifies the number of seconds that the system remains in the quiet state following a failed authentication exchange with the client; valid values are from 0 to 65535 seconds.
<b>tx-period</b> <i>seconds</i>	Specifies the number of seconds that the system waits for a response to an EAP-request/identity frame from the client before retransmitting the request; valid values are from 30 to 65535 seconds.
<b>supp-timeout</b> <i>seconds</i>	Specifies the number of seconds that the system waits for the retransmission of EAP-request packets; valid values are from 30 to 65535 seconds.
<b>server-timeout</b> <i>seconds</i>	Specifies the number of seconds that the system waits for the retransmission of packets by the back-end authenticator to the authentication server; valid values are from 30 to 65535 seconds.

## Defaults

The defaults are as follows:

- **reauth-period** is **3600** seconds.
- **quiet-period** is **60** seconds.
- **tx-period** is **30** seconds.
- **supp-timeout** is **30** seconds.
- **server-timeout** is **30** seconds.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

You must enable periodic reauthentication before you enter the **dot1x timeout reauth-period** command. Enter the **dot1x reauthentication** command to enable periodic reauthentication. The **dot1x timeout reauth-period** command affects the behavior of the system only if periodic reauthentication is enabled.

**Examples**

This example shows how to set the number of seconds between reauthentication attempts to 4000:

```
Router(config-if)# dot1x timeout reauth-period 4000
Router(config-if)#
```

This example shows how to set the quiet time on the system to 30 seconds:

```
Router(config-if)# dot1x timeout quiet-period 30
Router(config-if)#
```

This example shows how to set 60 as the number of seconds to wait for a response to an EAP-request/identity frame from the client before retransmitting the request:

```
Router(config-if)# dot1x timeout tx-period 60
Router(config-if)#
```

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

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

This example shows how to set the system-to-authentication-server retransmission time for transport layer packets to 25 seconds:

```
Router(config-if)# dot1x timeout server-timeout 25
Router(config-if)#
```

This example shows how to return to the default reauthorization period:

```
Router(config-if)# no dot1x timeout reauth-period
Router(config-if)#
```

**Related Commands**

Command	Description
<b>dot1x reauthentication</b>	Enables periodic reauthentication of the client.
<b>show dot1x</b>	Displays 802.1X information.

# duplex

To configure the duplex operation on an interface, use the **duplex** command. To return the system to half-duplex mode, use the **no** form of this command.

**duplex { full | half }**

**no duplex**

Syntax Description	full	Specifies full-duplex operation.
	half	Specifies half-duplex operation.

Defaults	<b>half</b>
----------	-------------

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** [Table 2-7](#) lists the supported command options by interface.

**Table 2-7 Supported duplex Command Options**

Interface Type	Supported Syntax	Default Setting	Usage Guidelines
10/100-Mbps module	<b>duplex [half   full]</b>	See the “Usage Guidelines” section.	If the speed is set to <b>auto</b> , you will not be able to set <b>duplex</b> . If the speed is set to <b>10</b> or <b>100</b> , and you do not configure the duplex setting, the duplex is set to <b>half</b> .
100-Mbps fiber modules	<b>duplex [half   full]</b>	<b>half</b>	—
Gigabit Ethernet Interfaces	<b>duplex full</b>	<b>full</b>	—
10-Mbps ports	<b>duplex [half   full]</b>	<b>half</b>	—

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 half duplex. You must configure the correct duplex mode when the transmission speed is changed to 10 or 100 from 1000.

Gigabit Ethernet is full duplex only. You cannot change the duplex mode on Gigabit Ethernet ports or on a 10/100/1000-Mbps port that is configured for Gigabit Ethernet.

When manually configuring the interface speed to either 10 or 100 Mbps, you should also configure the duplex mode on the interface.

**Note**

Catalyst 6500 series switches cannot automatically negotiate the interface speed and duplex mode if either connecting interface is configured to a value other than **auto**.

**Caution**

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

Table 2-8 describes the relationship and the results for the different combinations of the **duplex** and **speed** commands.

**Table 2-8 Relationship Between duplex and speed Commands**

duplex Command	speed Command	Resulting System Action
<b>duplex half</b> or <b>duplex full</b>	<b>speed auto</b>	Autonegotiates both speed and duplex modes
<b>duplex half</b>	<b>speed 10</b>	Forces 10 Mbps and half duplex
<b>duplex full</b>	<b>speed 10</b>	Forces 10 Mbps and full duplex
<b>duplex half</b>	<b>speed 100</b>	Forces 100 Mbps and half duplex
<b>duplex full</b>	<b>speed 100</b>	Forces 100 Mbps and full duplex

**Examples**

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

```
Router(config-if)# duplex full
Router(config-if)#
```

**Related Commands**

Command	Description
<a href="#">interface</a>	Selects an interface to configure and enters interface configuration mode.
<b>show controllers</b>	Displays information that is specific to the hardware on a module.
<b>show interfaces</b>	Displays the traffic that is seen by a specific interface.
<a href="#">speed</a>	Sets the port speed for an Ethernet interface.

# eigrp event-log-size

To set the size of the IP-EIGRP event log, use the **eigrp event-log-size** command.

**eigrp event-log-size** *size*

<b>Syntax Description</b>	<i>size</i> IP-EIGRP event log size; valid values are from 0 to 4294967295.
---------------------------	---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	Once the configured event log size has been exceeded, the last configured (event-log-size) number of lines of log is retained.
-------------------------	--

<b>Examples</b>	This example shows how to set the size of the IP-EIGRP event log:
-----------------	---

```
Router (config-router)# eigrp event-log-size 5000010
Router (config-router)#
```

<b>Related Commands</b>	Command	Description
	<b>clear ip eigrp event</b>	Clears the IP-EIGRP event log.

# encapsulation dot1q

To enable the IEEE 802.1Q encapsulation of traffic on a specified subinterface in the VLANs, use the **encapsulation dot1q** command.

**encapsulation dot1q** *vlan-id* [**native**]

Syntax Description		
	<i>vlan-id</i>	Virtual LAN identifier; valid values are from 1 to 4094.
	<b>native</b>	(Optional) Sets the PVID value of the port to the <i>vlan-id</i> value.

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

**Command Modes** Subinterface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Always use the **native** keyword when the *vlan-id* is the ID of the 802.1Q native VLAN. Do not configure encapsulation on the native VLAN of an 802.1Q trunk without the **native** keyword.

To enter the subinterface configuration mode, you must enter the interface configuration mode first and then enter the **interface** command to specify a subinterface.

**Examples** This example shows how to set encapsulation for VLAN traffic using the 802.1Q protocol for VLAN 100:

```
Router(config-subif)# encapsulation dot1q 100
Router(config-subif)#
```

Related Commands	Command	Description
	<a href="#">encapsulation isl</a>	Enables ISL.

# encapsulation isl

To enable ISL, use the **encapsulation isl** command.

**encapsulation isl** *vlan-identifier*

<b>Syntax Description</b>	<i>vlan-identifier</i>	VLAN identifier; valid values are from 1 to 4094.
---------------------------	------------------------	---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	ISL is a Cisco protocol that is used for interconnecting multiple switches and routers and for defining VLAN topologies.
-------------------------	--

ISL encapsulation adds a 26-byte header to the beginning of the Ethernet frame. The header contains a 10-bit VLAN identifier that conveys VLAN membership identities between the switches.

To enter the subinterface configuration mode, you must enter the interface configuration mode first and then enter the **interface** command to specify a subinterface.

<b>Examples</b>	This example shows how to enable ISL on Fast Ethernet subinterface 2/1.20:
-----------------	--

```
Router(config-subif)# encapsulation isl 400
Router(config-subif)#
```

<b>Related Commands</b>	Command	Description
	<b>bridge-group</b>	Assigns each network interface to a bridge group.
<b>show bridge vlan</b>	Displays virtual LAN subinterfaces.	
<a href="#">show interfaces</a>	Displays the traffic that is seen by a specific interface.	
<a href="#">show vlans</a>	Displays information about the Cisco IOS VLAN subinterfaces.	

# erase

To erase a file system, use the **erase** command.

```
erase {const_nvram: | nvram: | startup-config:}
```

## Syntax Description

<b>const_nvram:</b>	Erases all files under the const_nvram: partition.
<b>nvram:</b>	Erases NVRAM.
<b>startup-config:</b>	Erases the contents of the configuration memory.

## Defaults

This command has no default settings.

## Command Modes

EXEC

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines



### Caution

When you use the **erase** command to erase a file system, you cannot recover the files in the file system.

The **erase nvram:** command replaces the **write erase** command and the **erase startup-config** command.

You can use the **erase** command on both Class B and Class C flash file systems only. To reclaim space on flash file systems after deleting files using the **delete** command, you must use the **erase** command. The **erase** command erases all of the files in the flash file system.

Class A flash file systems cannot be erased. You can delete individual files using the **delete** command and then reclaim the space using the **squeeze** command. You can also use the **format** command to format the flash file system.

On Class C flash file systems, space is dynamically reclaimed when you use the **delete** command. You can also use either the **format** or **erase** command to reinitialize a Class C flash file system.

The **erase nvram:** command erases NVRAM. On Class A file system platforms, if the CONFIG\_FILE variable specifies a file in flash memory, the specified file is marked “deleted.”

You can enter the **erase const\_nvram** command to erase the VLAN database configuration file.

**Examples**

This example shows how to erase the NVRAM and the startup configuration in the NVRAM:

```
Router# erase nvram:
Router#
```

**Related Commands**

Command	Description
<a href="#">boot config</a>	Specifies the device and filename of the configuration file from which the system configures itself during initialization (startup).
<b>delete</b>	Deletes a file from a flash memory device or NVRAM.
<b>more nvram:startup-config:</b>	Displays the startup configuration file contained in NVRAM or specified by the CONFIG-FILE environment variable.
<a href="#">show bootvar</a>	Displays information about the BOOT environment variable.
<b>undelete</b>	Recovers a file that is marked “deleted” on a flash file system.

## errdisable detect cause

To enable the error-disable detection, use the **errdisable detect cause** command. To disable the error-disable detection, use the **no** form of this command.

**errdisable detect cause** { **all** | **dtp-flap** | **l2ptguard** | **link-flap** | **packet-buffer-error** | **pagp-flap** | **udld** }

**no errdisable detect cause** { **all** | **dtp-flap** | **l2ptguard** | **link-flap** | **pagp-flap** | **udld** }

### Syntax Description

<b>all</b>	Specifies error-disable detection for all error-disable causes.
<b>dtp-flap</b>	Specifies detection for the DTP flap error-disable cause.
<b>l2ptguard</b>	Specifies detection for the Layer 2 protocol-tunnel error-disable cause.
<b>link-flap</b>	Specifies detection for the link flap error-disable cause.
<b>packet-buffer-error</b>	Causes the packet buffer error to error-disable the affected port.
<b>pagp-flap</b>	Specifies detection for the PAGP flap error-disable cause.
<b>udld</b>	Specifies detection for the UDLD error-disable cause.

### Defaults

Enabled for all causes.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines



#### Note

Entering the **no errdisable detect cause packet-buffer-error** command allows you to detect the fault that triggers a power cycle of the affected module.

A cause (bpduguard, dtp-flap, link-flap, pagp-flap, root-guard, udld) is defined as the reason why the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in an error-disabled state (an operational state that is similar to the link-down state).

You must enter the **shutdown** and then the **no shutdown** commands to recover an interface manually from the error-disable state.

---

**Examples**

This example shows how to enable the error-disable detection for the Layer 2 protocol-tunnel guard error-disable cause:

```
Router(config)# errdisable detect cause l2ptguard
Router(config)#
```

---

**Related Commands**

Command	Description
<a href="#">show errdisable detect</a>	Displays the error-disable detection status.
<a href="#">show interfaces status</a>	Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.

---

## errdisable recovery

To configure the recovery mechanism variables, use the **errdisable recovery** command. To return to the default state, 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 |
peseure-violation | security-violation | uddld | unicast-flood}
```

```
errdisable recovery {interval interval}
```

```
no errdisable recovery cause {all | {arp-inspection | bpduguard | channel-misconfig |
dhcp-rate-limit | dtp-flap | gbic-invalid | l2ptguard | link-flap | pagp-flap |
peseure-violation | security-violation | uddld | unicast-flood}}
```

```
no errdisable recovery {interval interval}
```

### Syntax Description

<b>cause</b>	Enables error-disable recovery to recover from a specific cause.
<b>all</b>	Enables the recovery timers for all error-disable causes.
<b>arp-inspection</b>	Enables error-disable recovery to recover from an ARP inspection cause.
<b>bpduguard</b>	Enables the recovery timer for the BPDU-guard error-disable cause.
<b>channel-misconfig</b>	Enables the recovery timer for the channel-misconfig error-disable cause.
<b>dhcp-rate-limit</b>	Enables the recovery timer for the DHCP rate-limit error-disable cause.
<b>dtp-flap</b>	Enables the recovery timer for the DTP-flap error-disable cause.
<b>gbic-invalid</b>	Enables the recovery timer for the GBIC invalid error-disable cause.
<b>l2ptguard</b>	Enables the recovery timer for the Layer 2 protocol-tunnel error-disable cause.
<b>link-flap</b>	Enables the recovery timer for the link-flap error-disable cause.
<b>pagp-flap</b>	Enables the recovery timer for the PAGP-flap error-disable cause.
<b>peseure-violation</b>	Enables the recovery timer for the peseure-violation error-disable cause.
<b>security-violation</b>	Enables the automatic recovery of ports that were disabled due to 802.1X security violations.
<b>uddld</b>	Enables the recovery timer for the UDLD error-disable cause.
<b>unicast-flood</b>	Enables the recovery timer for the unicast-flood error-disable cause.
<b>interval interval</b>	Specifies the time to recover from a specified error-disable cause; valid values are from 30 to 86400 seconds.

### Defaults

The defaults are as follows:

- Disabled for all causes.
- If enabled, the *interval* is 300 seconds.

### Command Modes

Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

The **secure-violation** option is not supported.

A cause (bpduguard, dhcp-rate-limit, dtp-flap, l2ptguard, link-flap, pagp-flap, security-violation, channel-misconfig, psecure-violation, udlld, or unicast-flood) is defined as the reason why the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in an error-disabled state (an operational state that is similar to the link-down state). If you do not enable errdisable recovery for the cause, the interface stays in the error-disabled state until a shutdown and no shutdown occurs. If you enable recovery for a cause, the interface is brought out of the error-disabled state and allowed to retry operation once all the causes have timed out.

You must enter the **shutdown** and then the **no shutdown** commands to recover an interface manually from the error-disabled state.

### Examples

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

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

This example shows how to set the timer to 300 seconds:

```
Router(config)# errdisable recovery interval 300
Router(config)#
```

### Related Commands

Command	Description
<a href="#">show errdisable recovery</a>	Displays the information about the error-disable recovery timer.
<a href="#">show interfaces status</a>	Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.

## error-detection packet-buffer action

To specify the action that a module takes after packet buffer memory failures, use the **error-detection packet-buffer action** command. To return to the default settings, use the **no** form of this command.

**error-detection packet-buffer action** { *module num* } { **error-disable** | **power-down** | **reset** }

Syntax Description	Parameter	Description
	<b>module num</b>	Specifies the module number.
	<b>error-disable</b>	Error disables the module.
	<b>power-down</b>	Powers down the module.
	<b>reset</b>	Resets the module.

**Defaults** Error-disable port group

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command is supported on the following modules only:

- WS-X6348-RJ-45
- WS-X6348-RJ-21V
- WS-X6248-RJ-45
- WS-X6248-TEL
- WS-X6148-RJ-45
- WS-X6148-RJ-21

When you specify the **reset** keyword, a rapid reboot (approximately 10 seconds) and not a normal reboot (approximately 45 to 50 seconds) is performed. Prior to this release, the module always went through a non-rapid reboot.

## Examples

This example shows how to set the module to error disable after packet buffer memory failures:

```
Router(config)# error-detection packet-buffer action module 2 error-disable
Router(config)#
```

This example shows how to set the module to power down after packet buffer memory failures:

```
Router(config)# error-detection packet-buffer action module 2 power-down
Router(config)#
```

This example shows how to set the module to reset after packet buffer memory failures:

```
Router(config)# error-detection packet-buffer action module 2 reset
Router(config)#
```

# file verify auto

To verify the compressed Cisco IOS image checksum, use the **file verify auto** command. To turn off automatic verification after a copy operation, use the **no** form of this command.

**file verify auto**

**no file verify auto**

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

**Defaults** Verification is done automatically after completion of a copy operation.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Enter the **copy /noverify** command to override the default behavior for a single copy operation.

**Examples** This example shows how to verify the compressed Cisco IOS image checksum:

```
Router(config)# file verify auto
Router(config)#
```

Related Commands	Command	Description
	<b>copy /noverify</b>	Disables the automatic image verification for the current copy operation.
	<b>verify</b>	Verifies the checksum of a file on a flash memory file system or computes an MD5 signature for a file.

# flowcontrol

To configure a port to send or receive pause frames, use the **flowcontrol** command.

**flowcontrol** {**send** | **receive**} {**desired** | **off** | **on**}

Syntax Description	send	receive	desired	off	on
	Specifies that a port sends pause frames.	Specifies that a port processes pause frames.	Obtains predictable results regardless of whether a remote port is set to <b>on</b> , <b>off</b> , or <b>desired</b> .	Prevents a local port from receiving and processing pause frames from remote ports or from sending 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.

## Defaults

Flow-control defaults depend upon port speed. The defaults are as follows:

- Gigabit Ethernet ports default to **off** for receive and **desired** for send.
- Fast Ethernet ports default to **off** for receive and **on** for send.
- On the 24-port 100BASE-FX and 48-port 10/100 BASE-TX RJ-45 modules, the default is **off** for receive and **off** for send.
- 10-Gigabit Ethernet ports are permanently configured to respond to pause frames, and the default for send is **off**.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

The **send** and **desired** keywords are supported on Gigabit Ethernet ports only.

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

Gigabit Ethernet ports on the Catalyst 6500 series switches use flow control to inhibit the transmission of packets to the port for a period of time; other Ethernet ports use flow control to respond to flow-control requests.

If a Gigabit Ethernet port receive buffer becomes full, the port transmits a “pause” packet that tells remote ports to delay sending more packets for a specified period of time. All Ethernet ports (1000 Mbps, 100 Mbps, and 10 Mbps) can receive and act upon “pause” packets from other devices.

You can configure non-Gigabit Ethernet ports to ignore received pause frames (**disable**) or to react to them (**enable**).

When used with **receive**, the **on** and **desired** keywords have the same result.

All Catalyst 6500 series switch Gigabit Ethernet ports can receive and process pause frames from remote devices.

To obtain predictable results, follow these guidelines:

- Use **send on** only when remote ports are set to **receive on** or **receive desired**.
- Use **send off** only when remote ports are set to **receive off** or **receive desired**.
- Use **receive on** only when remote ports are set to **send on** or **send desired**.
- Use **send off** only when remote ports are set to **receive off** or **receive desired**.

### Examples

These examples show how to configure the local port to not support any level of flow control by the remote port:

```
Router(config-if)# flowcontrol receive off
Router(config-if)#
```

```
Router(config-if)# flowcontrol send off
Router(config-if)#
```

### Related Commands

Command	Description
<a href="#">show interfaces flowcontrol</a>	Displays flow-control information.

# format

To format a Class A or Class C flash file system, use the **format** command.

Class A flash file system:

```
format bootflash: [spare spare-number] filesystem1: [[filesystem2:][monlib-filename]]
```

Class C flash file system:

```
format filesystem1:
```



## Caution

Reserve a certain number of memory sectors as spares, so that if some sectors fail, most of the flash PC card can still be used. Otherwise, you must reformat the flash PC card when some of the sectors fail.

## Syntax Description

<b>spare</b> <i>spare-number</i>	(Optional) Specifies the number of the spare sectors to reserve on formatted flash memory; valid values are from 0 to 16.
<i>filesystem1</i> :	File system to format; valid values are <b>disk0:</b> , <b>bootdisk:</b> , and <b>sup-bootdisk:</b> ; see the “Usage Guidelines” section for additional information.
<i>filesystem2</i> :	(Optional) File system containing the monlib file to use for formatting <i>filesystem1</i> followed by a colon.
<i>monlib-filename</i>	(Optional) Name of the ROM monitor library file (monlib file) to use for formatting the <i>filesystem1</i> argument.

## Defaults

The defaults are as follows:

- *monlib-filename* is the one bundled with the system software.
- *spare-number* is zero (0).

## Command Modes

EXEC

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

Use this command to format Class A or C flash memory file systems.

The Supervisor Engine 32 PISA has these flash memory devices:

- **disk0:**
  - One external CompactFlash Type II slot
  - Supports CompactFlash Type II Flash PC cards
- **sup-bootdisk:**
  - Supervisor Engine 32 PISA 256-MB internal CompactFlash flash memory
  - From the Supervisor Engine 32 PISA ROMMON, it is bootdisk:
- **bootdisk:**
  - PISA 256-MB internal CompactFlash flash memory
  - Not accessible from the Supervisor Engine 32 PISA ROMMON

In some cases, you might need to insert a new flash PC card and load images or back up configuration files onto it. Before you can use a new flash PC card, you must format it.

Sectors in flash PC cards can fail. Reserve certain flash PC sectors as “spares” by using the optional *spare* argument on the **format** command to specify between 0 and 16 sectors as spares. If you reserve a small number of spare sectors for emergencies, you can still use most of the flash PC card. If you specify 0 spare sectors and some sectors fail, you must reformat the flash PC card, which erases all existing data.

The monlib file is the ROM monitor library. The ROM monitor uses this file to access files in the flash file system. The Cisco IOS system software contains a monlib file.

When used with HSA and you do not specify the *monlib-filename* argument, the system takes the ROM monitor library file from the slave image bundle. If you specify the *monlib-filename* argument, the system assumes that the files reside on the slave devices.

In the command syntax, *filesystem1:* specifies the device to format, and *filesystem2:* specifies the optional device containing the monlib file, used to format *filesystem1:*. If you omit the optional *filesystem2:* and *monlib-filename* arguments, the system formats *filesystem1:*, using the monlib file that is already bundled with the system software. If you omit only the optional *filesystem2:* argument, the system formats *filesystem1:*, using the monlib file from the device that you specified with the **cd** command. If you omit only the optional *monlib-filename* argument, the system formats *filesystem1:* using *filesystem2:*'s monlib file. When you specify both arguments—*filesystem2:* and *monlib-filename*—the system formats *filesystem1:*, using the monlib file from the specified device. You can specify *filesystem1:*'s own monlib file in this argument. If the system cannot find a monlib file, it terminates its formatting.

**Examples**

This example shows how to format a CompactFlash PC card that is inserted in slot 0:

```
Router# format disk0:
Running config file on this device, proceed? [confirm]y
All sectors will be erased, proceed? [confirm]y
Enter volume id (up to 34 characters): <Return>
Formatting sector 4 (erasing)
Format device disk0 completed
```

When the console returns to the EXEC prompt, the new CompactFlash PC card is successfully formatted and ready for use.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>cd</b>	Changes the default directory or file system.
<b>copy</b>	Copies any file from a source to a destination.
<b>delete</b>	Deletes a file from a flash memory device or NVRAM.
<b>show file systems</b>	Lists available file systems.
<b>undelete</b>	Recovers a file that is marked as “deleted” on a flash file system.

# fsck

To check a flash file system for damage and to repair any problems, use the **fsck** command.

**fsck** [/automatic | disk0:]

Syntax Description	
<b>/automatic</b>	(Optional) Specifies automatic mode; see the “Usage Guidelines” section for additional information.
<b>disk0:</b>	(Optional) Specifies the file system to check.

**Defaults** The current file system is checked if **disk0:** is not specified.

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command is valid only on Class C flash file systems and on PCMCIA ATA flash disks and CompactFlash disks.

If you do not enter any arguments, the current file system is used. Use the **pwd** command to display the current file system.

If you enter the **disk0:** keyword, the fsck utility checks the selected file system for problems. If a problem is detected, a prompt is displayed asking if you want the problem fixed.

If you enter the **/automatic** keyword, you are prompted to confirm that you want the automatic mode. In automatic mode, problems are fixed automatically and you are not prompted to confirm.

Table 2-9 lists the checks and actions that are performed by the fsck utility.

**Table 2-9 fsck Utility Checks and Actions**

Checks	Actions
Checks the boot sector and the partition table and reports the errors.	No action.
Validates the media with the signature in the last 2 bytes of the first sector (0x55 and 0xaa, respectively).	No action.
Checks the os_id to find whether this is a FAT-12 or FAT-16 file system (valid values include 0, 1, 4, and 6).	No action.
Checks the number of FAT's field (correct values are 1 and 2).	No action.

Table 2-9 fsck Utility Checks and Actions (continued)

Checks	Actions
Checks these values: <ul style="list-style-type: none"> <li>• n_fat_sectors cannot be less than 1.</li> <li>• n_root_entries cannot be less than 16.</li> <li>• n_root_sectors cannot be less than 2.</li> <li>• base_fat_sector, n_sectors_per_cluster, n_heads, n_sectors_per_track is not 0.</li> </ul>	No action.
Checks the files and FAT for these errors:	
Checks the FAT for invalid cluster numbers.	If the cluster is a part of a file chain, the cluster is changed to end of file (EOF). If the cluster is not part of a file chain, it is added to the free list and unused cluster chain. <a href="#">Table 2-10</a> lists valid cluster numbers; numbers other than those listed in <a href="#">Table 2-10</a> are invalid numbers.
Checks the file's cluster chain for loops.	If the loop is broken, the file is truncated at the cluster where the looping occurred.
Checks the directories for nonzero size fields.	If directories are found with nonzero size fields, the size is reset to zero.
Checks for invalid start cluster file numbers.	If the start cluster number of a file is invalid, the file is deleted.
Checks files for bad or free clusters.	If the file contains bad or free clusters, the file is truncated at the last good cluster; an example is the cluster that points to this bad/free cluster.
Checks to see if the file's cluster chain is longer than indicated by the size fields.	If the file's cluster chain is longer than indicated by the size fields, the file size is recalculated and the directory entry is updated.
Checks to see if two or more files share the same cluster (crosslinked).	If two or more files are crosslinked, you are prompted to accept the repair, and one of the files is truncated.
Checks to see if the file's cluster chain is shorter than is indicated by the size fields.	If the file's cluster chain is shorter than is indicated by the size fields, the file size is recalculated and the directory entry is updated.
Checks to see if there are any unused cluster chains.	If unused cluster chains are found, new files are created and linked to that file with the name <i>fsck-start cluster</i> .

**Table 2-10 Valid Cluster Numbers**

Cluster	FAT-12	FAT-16
Next entry in the chain	2-FEF	2-FFE
Last entry in chain	FF8-FFF	FFF8-FFFF
Available cluster	0	0
Bad cluster	FF7	FFF7

**Examples**

This example shows how to run a check of the current file system:

```

Router# fsck
Checking the boot sector and partition table111
Checking FAT, Files and Directories111
Files
4) disk0:/FILE3 and
5) disk0:/FILE5
have a common cluster1
Press 4/5 to truncate or any other character to ignore[confirm] q
Ignoring this error and continuing with the rest of the check111
Files
4) disk0:/FILE5 and
5) disk0:/FILE4
have a common cluster1
Press 4/5 to truncate or any other character to ignore[confirm] 1
File disk0:/FILE5 truncated1
Files
4) disk0:/FILE7 and
5) disk0:/FILE6
have a common cluster1
1
1
1
4) disk0:/FILE45 and
5) disk0:/FILE43
have a common cluster1
Press 4/5 to truncate or any other character to ignore[confirm] i
Ignoring this error and continuing with the rest of the check111
Reclaiming unused space111
Created file disk0:/fsck-44 for an unused cluster chain
Created file disk0:/fsck-50 for an unused cluster chain
Created file disk0:/fsck-30 for an unused cluster chain
Created file disk0:/fsck-35 for an unused cluster chain
Created file disk0:/fsck-40 for an unused cluster chain
Created file disk0:/fsck-46 for an unused cluster chain
Created file disk0:/fsck-55 for an unused cluster chain
Created file disk0:/fsck-65 for an unused cluster chain
Created file disk0:/fsck-90 for an unused cluster chain
Updating FAT111
fsck of disk0: complete
Router#

```

# hold-queue

To limit the size of the IP output queue on an interface, use the **hold-queue** command. To return to the default settings, use the **no** form of this command.

**hold-queue** *length* {**in** | **out**}

**no hold-queue** {**in** | **out**}

Syntax Description		
	<i>length</i>	Maximum number of packets in the queue; valid values are from 0 to 65535.
	<b>in</b>	Specifies the input queue.
	<b>out</b>	Specifies the output queue.

## Defaults

The defaults are as follows:

- The input hold-queue limit is 75 packets.
- The default output hold-queue limit is 40 packets.
- The default is 10 packets for asynchronous interfaces.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

This command is not supported on the OSM.

The default limits prevent a malfunctioning interface from consuming an excessive amount of memory. There is no fixed upper limit to a queue size.

The default of ten packets allows the Cisco IOS software to queue a number of back-to-back routing updates. The default is for asynchronous interfaces only; other media types have different defaults.

The guidelines for hold queues and priority queueing are as follows:

- The hold queue stores packets that are received from the network and are waiting to be sent to the client. We recommend that the queue size does not exceed ten packets on asynchronous interfaces. For most other interfaces, the queue length should not exceed 100 packets.
- The input hold queue prevents a single interface from flooding the network server with too many input packets. Additional input packets are discarded if the interface has too many outstanding input packets in the system.
- If you use priority output queueing, you can set the length of the four output queues using the **priority-list** global configuration command. You cannot use the **hold-queue** command to set an output hold-queue length in this situation.
- For slow links, use a small output hold-queue limit to prevent storing packets at a rate that exceeds the transmission capability of the link.

- For fast links, use a large output hold-queue limit. A fast link may be busy for a short time (and require the hold queue) but can empty the output hold queue quickly when capacity returns.
- You can display the current hold-queue setting and the number of packets that are discarded because of hold-queue overflows by using the **show interfaces** command in EXEC mode.

**Caution**


---

Increasing the hold queue can cause negative effects to network routing and response times. If you use protocols that have sequence/acknowledge packets to determine round-trip times, do not increase the output queue. Instead, we recommend that you program the Catalyst 6500 series switch to drop packets and inform the hosts to slow down transmissions to match the available bandwidth. We do not recommend that you make duplicate copies of the same packet within the network.

---

**Examples**

This example sets a small input queue on a slow serial line:

```
Router(config)# interface serial 0
Router(config-if)# hold-queue 30 i
```

**Related Commands**

Command	Description
<b>priority-list</b>	Establishes queueing priorities based on the protocol type.
<b>show interfaces</b>	Displays the traffic that is seen by a specific interface.

## hw-module boot

To specify the boot options for the module through the power management bus control register, use the **hw-module boot** command.

```
hw-module {module num} {boot [value] {config-register | eobc | {flash image} | rom-monitor}}
```

Syntax Description	module num	Specifies the number of the module to apply the command.
	value	(Optional) Literal value for the module's boot option; valid values are from 0 to 15. See the "Usage Guidelines" section for additional information.
	config-register	Boots using the module's config-register value.
	eobc	Boots using an image downloaded through EOBC.
	flash image	Specifies the image number in the module's internal flash memory for the module's boot option; valid values are 1 and 2.
	rom-monitor	Stays in ROM-monitor mode after the module resets.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command is supported on the CMM only.

The valid values for the **boot value** argument are as follows:

- 0—Specifies the module's config-register value.
- 1—Specifies the first image in the flash memory.
- 2—Specifies the second image in the flash memory.
- 3—Stays in ROM-monitor mode after the module reset.
- 4—Specifies the download image through EOBC.

**Examples** This example shows how to reload the module in slot 6 using the module's config-register value:

```
Router# hw-module slot 1/6 boot config-register
Router#
```

This example shows how to reload the module in slot 3 using an image downloaded through EOBC:

```
Router# hw-module slot 1/3 boot eobc
Router#
```

## hw-module fan-tray version

To set the fan-type (high or low power) version, use the **hw-module fan-tray version** command.

**hw-module fan-tray version [1 | 2]**

<b>Syntax Description</b>	<b>1   2</b> (Optional) Specifies the version number; see the “Usage Guidelines” section for additional information.
---------------------------	--

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

**Command Modes** Privileged EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Before you install a high-capacity fan tray, enter the **hw-module fan-tray version 2** command to check for configuration problems, such as power-supply compatibility and power sufficiency. If there are no problems, a message is displayed to change the fan tray from version 1 to version 2. At this point, you can remove the old fan tray and quickly insert the new high-capacity fan tray.

This command is supported on the following chassis:

- WS-C6506
- WS-C6509
- WS-C6509-NEB/OSR7609

Set the version to **2** before installing higher power fan trays. Set the version to **1** before downgrading to lower power fan trays.

Command confirmation does not change the fan power consumption or cooling capacity. It updates the backplane IDPROM. The new values take effect the next time that you insert a fan.

When you execute the command, the software checks the configurations and prompts for confirmation. Any illegal configurations (such as power-supply incompatibility) result in a warning being displayed and a command failure.

**Examples** This example shows how to set the fan type for lower power fan trays:

```
Router # hw-module fan-tray version 1
Router #
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show environment cooling</a>	Displays information about the cooling parameter.

# hw-module oversubscription

To administratively disable the oversubscribed ports (3, 4, 7, and 8) on a module, use the **hw-module oversubscription** command. Use the **no** form of this command to enable the oversubscribed ports.

**hw-module {module num} oversubscription**

**no hw-module {module num} oversubscription**

Syntax Description	<b>module num</b>	Applies the command to a specific module.
--------------------	-------------------	---

Defaults	Enabled.
----------	----------

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Usage Guidelines	<p>This command is supported on the WS-X6708-10G-3C and the WS-X6708-10G-3CXL modules only.</p> <p>When you disable the oversubscribed ports, the port is put into shutdown mode. In this mode, you cannot enter the <b>no shut</b> command on the disabled ports. If you attempt to enter the <b>no shut</b> command on the disabled ports, this message appears:</p>
------------------	--

The current module is operating in non-oversubscription mode! To utilise this interface, enable oversubscription mode for the module!

The *num* argument designates the module number. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values for the module number are from 1 to 13.

When you enter the **show interfaces** command on the disabled ports, the output displays “disabled for performance” to distinguish between the normal port shutdown and the shutdown for performance.

Examples	This example shows how to administratively disable the oversubscribed ports on a module:
----------	--

```
Router # hw-module module 3 oversubscription
Router #
```

This example shows how to administratively enable the oversubscribed ports on a module:

```
Router # no hw-module module 3 oversubscription
Router #
```

Related Commands	Command	Description
	<a href="#">show interfaces</a>	Displays traffic that is seen by a specific interface.

# hw-module reset

To reset a module by turning the power off and then on, use the **hw-module reset** command.

**hw-module {module *num*} reset**

<b>Syntax Description</b>	<b>module <i>num</i></b> Applies the command to a specific module; see the “Usage Guidelines” section for valid values.
---------------------------	---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	The <i>num</i> argument designates the module number. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values for the module number are from 1 to 13.
-------------------------	---

<b>Examples</b>	This example shows how to reload a specific module:
-----------------	---

```
Router # hw-module module 3 reset
Router #
```

# hw-module shutdown

To shut down the module, use the **hw-module shutdown** command.

**hw-module {module num} shutdown**

<b>Syntax Description</b>	<b>module num</b> Applies the command to a specific module; see the “Usage Guidelines” section for valid values.
---------------------------	--

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	<p>This command is supported on the SSL Services Module and the NAM.</p> <p>If you enter the <b>hw-module shutdown</b> command to shut down the module, you will have to enter the <b>no power enable module</b> command and the <b>power enable module</b> command to restart (power down and then power up) the module.</p>
-------------------------	---

<b>Examples</b>	This example shows how to shut down and restart the module:
-----------------	---

```
Router# hw-module module 3 shutdown
Router# no power enable module 3
Router# power enable module 3
```

## hw-module simulate link-up

To enable a software link on a specified module, use the **hw-module simulate link-up** command. For information on disabling a software link, refer to the “Usage Guidelines” section.

**hw-module {module num} simulate link-up**

<b>Syntax Description</b>	<b>module num</b>	Applies the command to a specific module; see the “Usage Guidelines” section for valid values.
---------------------------	-------------------	--

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	<p>This command is supported on Ethernet modules only.</p> <p>To disable a software link on a module, you must perform one of the following procedures:</p> <ul style="list-style-type: none"> <li>• Enter the <b>shutdown</b> and then the <b>no shutdown</b> commands on all the ports on the module.</li> <li>• Enter the <b>hw-module reset</b> command.</li> </ul> <p>When you apply this command to a module, the port LEDs on the module will glow green and simulate a link-up condition. This command can be used for testing interface configurations without cabling to the interface.</p> <p>The <i>num</i> argument designates the module number. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values for the module number are from 1 to 13.</p>
-------------------------	--

<b>Examples</b>	This example shows how to enable softlink on a module:
-----------------	--

```
Router# hw-module module 3 simulate link-up
Router#
```

Related Commands	Command	Description
	<b>hw-module reset</b>	Resets a module by turning the power off and then on.

# instance

To map a VLAN or a set of VLANs to an MST instance, use the **instance** command. To return the VLANs to the default instance (CIST), use the **no** form of this command.

```
instance instance-id { vlan vlan-range }
```

```
no instance instance-id
```

Syntax Description	
<i>instance-id</i>	Instance to which the specified VLANs are mapped; valid values are from 0 to 4094.
<b>vlan</b> <i>vlan-range</i>	Specifies the number of the VLANs to be mapped to the specified instance; valid values are from 1 to 4094.

**Defaults** No VLANs are mapped to any MST instance (all VLANs are mapped to the CIST instance).

**Command Modes** MST configuration submode

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **vlan** *vlan-range* is entered as a single value or a range. The mapping is incremental, not absolute. When you enter a range of VLANs, this range is added or removed to the existing instances. Any unmapped VLAN is mapped to the CIST instance. You can configure up to 65 interfaces

**Examples** This example shows how to map a range of VLANs to instance 2:

```
Router(config-mst)# instance 2 vlan 1-100
Router(config-mst)#
```

This example shows how to map a VLAN to instance 5:

```
Router(config-mst)# instance 5 vlan 1100
Router(config-mst)#
```

This example shows how to move a range of VLANs from instance 2 to the CIST instance:

```
Router(config-mst)# no instance 2 vlans 40-60
Router(config-mst)#
```

This example shows how to move all the VLANs that are mapped to instance 2 back to the CIST instance:

```
Router(config-mst)# no instance 2
Router(config-mst)#
```

#### Related Commands

Command	Description
<b>name (MST configuration submode)</b>	Sets the name of an MST region.
<b>revision</b>	Sets the revision number for the MST configuration.
<b>show</b>	Verifies the MST configuration.
<b>show spanning-tree mst</b>	Displays the information about the MST protocol.
<b>spanning-tree mst configuration</b>	Enters MST-configuration submode.

# interface

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

```
interface {type module} [.subinterface]
```

Syntax Description	<i>type</i>	Type of interface to be configured; see <a href="#">Table 2-11</a> for valid values.
	<i>module</i>	Module and port number or port-subinterface number; see the “Usage Guidelines” section for additional information.
	<i>.subinterface</i>	(Optional) Subinterface number to be configured; valid values are from 0 to 4294967295.

**Defaults** No interface types are configured.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** [Table 2-11](#) lists the valid values for *type*.

**Table 2-11 Valid type Values**

Keyword	Definition
<b>fastethernet</b>	100-Mbps Ethernet interface.
<b>gigabithernet</b>	Gigabit Ethernet IEEE 802.3z interface.
<b>tengigabithernet</b>	10-Gigabit Ethernet IEEE 802.3ae interface.
<b>ge-wan</b>	Gigabit Ethernet WAN IEEE 802.3z interface.
<b>pos</b>	Packet OC-3 interface on the Packet over SONET Interface Processor.
<b>atm</b>	ATM interface.
<b>vlan</b>	VLAN interface; see the <a href="#">interface vlan</a> command.
<b>port-channel</b>	Port channel interface; see the <a href="#">interface port-channel</a> command.
<b>null</b>	Null interface; the valid value is <b>0</b> .
<b>tunnel</b>	Tunnel interface.

By default, the Supervisor Engine 32 PISA EtherChannel (port channel interface 256, which is automatically configured with the **pisa-channel** command) is a 1-Gbps EtherChannel.

**Note**


---

The **pisa-channel** command is visible in the configuration file, but it is not user configurable.

---

You can enter the number of a port subinterface in the following format:

**interface** *{{type module/port.subinterface}}*

The Supervisor Engine 32 PISA ports are as follows:

- Supervisor Engine 32 PISA Management Ports—The console port for the Supervisor Engine 32 PISA port is an EIA/TIA-232 (RS-232) port. The Supervisor Engine 32 PISA also has two Universal Serial Bus (USB) 2.0 ports that currently are not enabled.
- Supervisor Engine 32 PISA Data Ports for the WS-S32-10GE-PISA has the following ports:
  - Ports 1 and 2: XENPAK 10 Gigabit Ethernet
  - Port 3: 10/100/1000 Mbps RJ-45

**Note**


---

You can disable Port 3 and reallocate its port ASIC capacity to the PISA EtherChannel (see the “Configuring Full PISA EtherChannel Bandwidth” section in the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*).

---

- Supervisor Engine 32 PISA Data Ports for the WS-S32-GE-PISA has these ports:
  - Ports 1 through 8: Small form-factor pluggable (SFP) Gigabit Ethernet
  - Port 9: 10/100/1000 Mbps RJ-45 port

**Note**


---

You can disable port 9 and reallocate its port ASIC capacity to the PISA EtherChannel (see the “Configuring Full PISA EtherChannel Bandwidth” section in the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*).

---

**Note**


---

After the port becomes a member of the PISA EtherChannel, only the **no channel-group 256 mode on** command has any effect on the port until the port is no longer a member of the PISA EtherChannel. While the port is a member of the PISA EtherChannel, all port configuration commands except the **no channel-group 256 mode on** command are ignored.

---

On a WS-S32-GE-PISA, you can allocate both ports 8 and 9 to the PISA EtherChannel.

You cannot enter any configuration under port channel interface 256.

The PISA EtherChannel MTU size is 4,096 bytes.

**Examples**

This example shows how to allocate the port ASIC capacity of port 3 to the PISA EtherChannel on a WS-S32-10GE-PISA that is installed in slot 5:

```
Router(config)# interface gigabitethernet 5/3
Router(config-if)# channel-group 256 mode on
Router(config-if)#
```

This example shows how to allocate the port ASIC capacity of port 9 to the PISA EtherChannel on a WS-S32-GE-PISA that is installed in slot 5:

```
Router(config)# interface gigabitethernet 5/9
Router(config-if)# channel-group 256 mode on
Router(config-if)#
```

This example shows how to revert to the default port ASIC capacity allocation.

```
Router(config)# interface gigabitethernet 5/9
Router(config-if)# no channel-group 256 mode on
Router(config-if)#
```

---

**Related Commands**

Command	Description
<a href="#">show interfaces</a>	Displays the traffic that is seen by a specific interface.

# interface port-channel

To create a port-channel virtual interface and enter interface configuration mode, use the **interface port-channel** command. To remove a virtual interface or subinterface, use the **no** form of this command.

**interface port-channel** *channel-number* [*.subinterface*]

**no interface port-channel** *channel-number* [*.subinterface*]

## Syntax Description

<i>channel-number</i>	Channel number assigned to this port-channel interface; valid values are from 1 to 256.
<i>.subinterface</i>	(Optional) Subinterface number to be configured; valid values are from 0 to 4294967295.

## Defaults

This command has no default settings.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

This command is not supported on the IDSM and NAM.

This command is supported on EtherChannel, Fast EtherChannel, Gigabit EtherChannel, and 10-Gigabit EtherChannel interfaces.

The *channel-number* argument can be from 1 to 256, with a maximum of 128 port-channel interfaces.

You can create Layer 2 port channels dynamically or by entering the **interface port-channel** command; you can create Layer 3 port channels by entering the **interface port-channel** command only. You cannot create Layer 3 port channels dynamically.

Only one port channel in a channel group is allowed.

Ports can be bundled across any module.



### Caution

The Layer 3 port-channel interface is the routed interface. Do not enable Layer 3 addresses on the physical Fast Ethernet interfaces.

When you use the **interface port-channel** command, follow these guidelines:

- If you configure ISL, you must assign the IP address to the SVI.
- If you want to use CDP, you must configure it only on the physical Fast Ethernet interface and not on the port-channel interface.

- If you do not assign a static MAC address on the port-channel interface, a MAC address is automatically assigned. If you assign a static MAC address and then later remove it, the MAC address is automatically assigned.

### Examples

This example shows how to create a port-channel interface with a channel-group number of 256:

```
Router(config)# interface port-channel 256
Creating a switch port Po5561 channel-group 556 is L5
Router(config-if)#
```



#### Note

The port-channel interface counters that are shown by the **show counters interface port-channel** and **show interface port-channel counters** commands are not supported for channel groups that are using GE-WAN interfaces for QinQ link bundling. The **show interface port-channel** {*number* | *number.subif*} command (without the **counters** keyword) is supported, however.

### Related Commands

Command	Description
<b>channel-group</b>	Assigns and configures an EtherChannel interface to an EtherChannel group.
<b>show etherchannel</b>	Displays the EtherChannel information for a channel.

# interface range

To execute a command on multiple ports at the same time, use the **interface range** command.

```
interface range {port-range | {macro name}}
```

Syntax Description		
	<i>port-range</i>	Port range; for a list of valid values for <i>port-range</i> , see the “Usage Guidelines” section for additional information.
	<b>macro name</b>	Specifies the macro name.

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

**Command Modes** Global or interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The values that you entered with the **interface range vlan** command are applied to all existing VLAN SVIs.

Before you can use a macro, you must define a range using the **define interface-range** command.

All configuration changes that are made to a port range are saved to NVRAM, but port ranges that are created with the **interface range** command are not saved to NVRAM.

You can enter the port range in two ways:

- Specifying up to five port ranges
- Specifying a previously defined macro

You can either specify the ports or the name of a port-range macro. A port range must consist of the same port type, and the ports within a range cannot span slots.

You can define up to five port ranges on a single command with each range separated by a comma.

You can enter the range with or without white spaces. For example, you can enter the range as **gigabitethernet 7/1 -7** or **gigabitethernet 7/1-7**.

When you enter a range of VLANs, any SVIs that do not exist within that range are created.

When entering the *port-range*, use this format: *card-type* {*slot*}/{*first-port*} - {*last-port*}.

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

- **ethernet**
- **fastethernet**
- **gigabitethernet**
- **loopback**

- **tengigabitethernet**
- **tunnel**
- **ge-wan**
- **pos**
- **atm**
- **vlan** *vlan-id* (valid values are from 1 to 4094)
- **port-channel** *interface-number* (valid values are from 1 to 256)

You cannot specify both a macro and an interface range in the same command. After creating a macro, the CLI does not allow you to enter additional ranges. If you have already entered an interface range, the CLI does not allow you to enter a macro.

In addition, you can specify a single interface in *port-range*.

### Examples

This example shows how to execute a command on two port ranges:

```
Router(config)# interface range fastethernet 5/18 -20, ethernet 3/1 -24
Router(config-if-range)#
```

This command shows how to execute a port-range macro:

```
Router(config)# interface range macro macrol
Router(config-if-range)#
```

### Related Commands

Command	Description
<a href="#">define interface-range</a>	Creates an interface-range macro.
<a href="#">show running-config</a>	Displays the status and configuration of the module or Layer 2 VLAN.

# interface vlan

To create or access a dynamic SVI, use the **interface vlan** command. To delete an SVI, use the **no** form of this command.

**interface vlan** *vlan-id*

**no interface vlan** *vlan-id*

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

Defaults	Fast EtherChannel is not specified.
----------	-------------------------------------

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Usage Guidelines	SVIs are created the first time that you enter the <b>interface vlan</b> <i>vlan-id</i> command for a particular VLAN. The <i>vlan-id</i> value corresponds to the VLAN tag that is associated with the data frames on an ISL, the 802.1Q-encapsulated trunk, or the VLAN ID that is configured for an access port. A message displays whenever you create a new VLAN interface, so that you can check if you entered the correct VLAN number.
------------------	--

If you delete an SVI by entering the **no interface vlan** *vlan-id* command, the associated IDB pair is forced into an administrative down state and is marked as deleted. The deleted interface will not be visible in the **show interface** command.

You can reinstate a deleted SVI by entering the **interface vlan** *vlan-id* command for the deleted interface. The interface comes back up, but much of the previous configuration is gone.

VLANs 1006 to 1014 are internal VLANs on the Catalyst 6500 series switch and cannot be used for creating new VLANs.

Examples	This example shows the output when you enter the <b>interface vlan</b> <i>vlan-id</i> command for a new VLAN number:
----------	--

```
Router(config)# interface vlan 23
% Creating new VLAN interface1
Router(config)#
```

# inter-packet gap 6502-mode

To set the IPG value, use the **inter-packet gap 6502-mode** command. To return to the default settings, use the **no** form of this command.

**inter-packet gap 6502-mode**

**no inter-packet gap 6502-mode**

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

**Defaults** All fragments from flows that are received from an ACE with Layer 4 ports and permit action are permitted. All other fragments are dropped in the hardware. This action also applies to flows that are handled in the software regardless of this command setting.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command is supported on situations where a WS-X6704-10GE is connected to a WS-X6502-10GE only. You enter this command to change the IPG value of the WS-X6704-10GE to match the WS-X6502-10GE.

The default 6704 mode sets the IPG value to average 12. Based on packet size, the IPG between successive packets range from 9 to 15.

The 6502 mode sets the IPG value to average 16. Based on packet size, the IPG between successive packets range from 13 to 19.

**Examples** This example shows how to set the IPG to 6502 mode:

```
Router(config-if)# inter-packet gap 6502-mode
Router(config-if)#
```

This example shows how to set the IPG to the default mode:

```
Router(config-if)# no inter-packet gap 6502-mode
Router(config-if)#
```

# ip access-list hardware permit fragments

To permit all noninitial fragments in the hardware, use the **ip access-list hardware permit fragments** command. To return to the default settings, use the **no** form of this command.

**ip access-list hardware permit fragments**

**no ip access-list hardware permit fragments**

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

**Defaults** All fragments from flows that are received from an ACE with Layer 4 ports and permit action are permitted. All other fragments are dropped in the hardware. This action also applies to flows that are handled in the software regardless of this command setting.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Flow fragments that match ACEs with Layer 4 ports and permit results are permitted in the hardware, and all other fragments are dropped. An entry is added in the TCAM for each ACE with Layer 4 ports and permit action. This action could cause large ACLs to not fit in the TCAM. If this situation occurs, use the **ip access-list hardware permit fragments** command to permit all noninitial fragments in the hardware.

This command affects all ACLs that are currently applied to interfaces and not only newly-applied ACLs.

The initial flow fragments that match the ACEs with Layer 4 ports and permit results are permitted in the hardware. All other initial fragments are dropped in the hardware.

**Examples** This example shows how to permit all noninitial fragments in the hardware:

```
Router(config)# ip access-list hardware permit fragments
Router(config)#
```

This example shows how to return to the default settings:

```
Router(config)# no ip access-list hardware permit fragments
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show ip interface</a>	Displays the usability status of interfaces that are configured for IP.

## 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	
<i>arp-acl-name</i>	Access control list name.
<i>vlan-range</i>	VLAN number or range; valid values are from 1 to 4094.
<b>static</b>	(Optional) Treats implicit denies in the ARP ACL as explicit denies and drops packets that do not match any previous clauses in the ACL.

**Defaults** No defined ARP ACLs are applied to any VLAN.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** For *vlan-range*, you can specify the VLAN to which the switches and hosts belong. You can specify a single VLAN identified by a VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma.

When an ARP access control list is applied to a VLAN for dynamic ARP inspection, the ARP packets containing only the IP-to-Ethernet MAC bindings are compared against the ACLs. All other packet types are bridged in the incoming VLAN without validation.

This command specifies that the incoming ARP packets are compared against the ARP access control list, and the packets are permitted only if the access control list permits them.

If the access control lists deny the packets because of explicit denies, the packets are dropped. If the packets are denied because of an implicit deny, they are then matched against the list of DHCP bindings if the ACL is not applied statically.

If you do not specify the **static** keyword, it means that there is no explicit deny in the ACL that denies the packet, and DHCP bindings determine whether a packet is permitted or denied if the packet does not match any clauses in the ACL.

**Examples**

This example shows how to apply the ARP ACL static hosts to VLAN 1 for DAI:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z
Router(config)# ip arp inspection filter static-hosts vlan 1
Router(config)#
```

**Related Commands**

Command	Description
<a href="#">arp access-list</a>	Configures an ARP ACL for ARP inspection and QoS filtering and enters the ARP ACL configuration submenu.
<a href="#">show ip arp inspection</a>	Displays the status of DAI for a specific range of VLANs.

# ip arp inspection limit

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 return to the default settings, use the **no** form of this command.

```
ip arp inspection limit {rate pps [{burst interval seconds}]} ;none
```

```
no ip arp inspection limit
```

## Syntax Description

<b>rate pps</b>	Specifies the upper limit on the number of incoming packets processed per second; valid values are from 1 to 2048 pps.
<b>burst interval seconds</b>	(Optional) Specifies the consecutive interval in seconds over which the interface is monitored for the high rate of the ARP packets; valid values are from 1 to 15 seconds.
<b>none</b>	Specifies that there is no upper limit on the rate of the incoming ARP packets that can be processed.

## Defaults

The default settings are as follows:

- The **rate pps** 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 on all the trusted interfaces.
- The **burst interval seconds** is set to **1** second.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

You should configure the trunk ports with higher rates to reflect their aggregation. When the rate of the incoming packets exceeds the user-configured rate, the interface is placed into an error-disabled state. You can use the error-disable timeout feature to remove the port from the error-disabled state. The rate applies to both the trusted and nontrusted interfaces. Configure appropriate rates on trunks to handle the packets across multiple DAI-enabled VLANs, or use the **none** keyword to make the rate unlimited.

The rate of the incoming ARP packets on the channel ports is equal to the sum of the incoming rate of packets from all the channel members. Configure the rate limit for the channel ports only after examining the rate of the incoming ARP packets on the channel members.

After a switch receives more than the configured rate of packets every second consecutively over a period of burst seconds, the interface is placed into an error-disabled state.

**Examples**

This example shows how to limit the rate of the incoming ARP requests to 25 packets per second:

```
Router# config terminal
Router(config)# interface fa6/3
Router(config-if)# ip arp inspection limit rate 25
Router(config-if)#
```

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:

```
Router# config terminal
Router(config)# interface fa6/1
Router(config-if)# ip arp inspection limit rate 20 burst interval 5
Router(config-if)#
```

**Related Commands**

Command	Description
<a href="#">show ip arp inspection</a>	Displays the status of DAI 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	Parameter	Description
	<b>entries number</b>	Specifies the number of entries from the logging buffer; valid values are from 0 to 1024.
	<b>logs number</b>	Specifies the number of entries to be logged in an interval; valid values are from 0 to 1024.
	<b>interval seconds</b>	Specifies the logging rate; valid values are from 0 to 86400 (1 day).

### Defaults

The default settings are as follows:

- When dynamic ARP inspection is enabled, denied, or dropped, the ARP packets are logged.
- The **entries number** is **32**.
- The **logs number** is **5** per second.
- The **interval seconds** is **1** second.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

A **0** value for the **logs number** indicates that the entries should not be logged out of this buffer.

A **0** value for the **interval seconds** keyword and argument indicates an immediate log.

You cannot enter a **0** for both the **logs number** and the **interval seconds** keywords and arguments.

The first dropped packet of a given flow is logged immediately. The subsequent packets for the same flow are registered but are not logged immediately. Registration for these packets occurs in a log buffer that is shared by all the VLANs. Entries from this buffer are logged on a rate-controlled basis.

### Examples

This example shows how to configure the logging buffer to hold up to 45 entries:

```
Router# config terminal
Enter configuration commands, one per line! End with CNTL/]]
Router(config)# ip arp inspection log-buffer entries 45
Router(config)#
```

This example shows how to configure the logging rate for 10 logs per 3 seconds:

```
Router(config)# ip arp inspection log-buffer logs 10 interval 3
Router(config)#
```

Related Commands	Command	Description
	<a href="#">arp access-list</a>	Configures an ARP ACL for ARP inspection and QoS filtering and enters the ARP ACL configuration submode.
	<a href="#">clear ip arp inspection log</a>	Clears the status of the log buffer.
	<a href="#">show ip arp inspection log</a>	Shows the status of the log buffer.

# 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** This command has no default settings.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to configure an interface to be trusted:

```
Router# config terminal
Router(config)# interface fastEthernet 6/3
Router(config-if)# ip arp inspection trust
Router(config-if)#
```

Related Commands	Command	Description
	<a href="#">show ip arp inspection</a>	Displays the status of DAI for a specific range of VLANs.

## ip arp inspection validate

To perform specific checks for an ARP inspection, use the **ip arp inspection validate** command. To disable ARP inspection 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	Parameter	Description
	<b>src-mac</b>	(Optional) Checks the source MAC address in the Ethernet header against the sender's MAC address in the ARP body.
	<b>dst-mac</b>	(Optional) Checks the destination MAC address in the Ethernet header against the target MAC address in the ARP body.
	<b>ip</b>	(Optional) Checks the ARP body for invalid and unexpected IP addresses.

**Defaults** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses.

The **src-mac** checks are issued against both ARP requests and responses. The **dst-mac** checks are issued for ARP responses.



**Note** When enabled, packets with different MAC addresses are classified as invalid and are dropped.

When enabling the checks, specify at least one of the keywords (**src-mac**, **dst-mac**, and **ip**) on the command line. Each command overrides the configuration of the previous command. If a command enables **src** and **dst mac** validations, and a second command enables IP validation only, the **src** and **dst mac** validations are disabled as a result of the second command.

The **no** form of this command disables only the specified checks. If no check options are enabled, all the checks are disabled.

---

**Examples**

This example shows how to enable the source MAC validation:

```
Router(config)# ip arp inspection validate src-mac
Router(config)#
```

---

**Related Commands**

Command	Description
<a href="#">arp access-list</a>	Configures an ARP ACL for ARP inspection and QoS filtering and enters the ARP ACL configuration submenu.
<a href="#">show ip arp inspection</a>	Displays the status of DAI for a specific range of VLANs.

## ip arp inspection vlan

To enable 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*

<b>Syntax Description</b>	<i>vlan-range</i> VLAN number or range; valid values are from 1 to 4094.
---------------------------	--

<b>Defaults</b>	ARP inspection is disabled on all VLANs.
-----------------	--

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	<p>For <i>vlan-range</i>, you can specify a single VLAN identified by a VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma.</p> <p>You must specify on which VLANs to enable DAI. DAI may not function on the configured VLANs if the VLAN has not been created or is a private VLAN.</p>
-------------------------	--

<b>Examples</b>	This example shows how to enable DAI on VLAN 1:
-----------------	---

```
Router(config)# ip arp inspection vlan 1
Router(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">arp access-list</a>	Configures an ARP ACL for ARP inspection and QoS filtering and enters the ARP ACL configuration submode.
	<a href="#">show ip arp inspection</a>	Displays the status of DAI 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

<i>vlan-range</i>	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.
<b>acl-match</b>	Specifies the logging criteria for packets that are dropped or permitted based on ACL matches.
<b>matchlog</b>	Specifies that logging of packets matched against ACLs is controlled by the <b>matchlog</b> keyword in the permit and deny access control entries of the ACL.
<b>none</b>	Specifies that ACL-matched packets are not logged.
<b>dhcp-bindings</b>	Specifies the logging criteria for packets dropped or permitted based on matches against the DHCP bindings.
<b>permit</b>	Specifies logging when permitted by DHCP bindings.
<b>all</b>	Specifies logging when permitted or denied by DHCP bindings.
<b>none</b>	Prevents all logging of packets permitted or denied by DHCP bindings.

## Defaults

All denied or dropped packets are logged.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

By default, the **matchlog** keyword is not available on the ACEs. When you enter the **matchlog** keyword, denied packets are not logged. Packets are logged only when they match against an ACE that has the **matchlog** keyword.

The **acl-match** and **dhcp-bindings** keywords merge with each other. When you set an ACL match configuration, the DHCP bindings configuration is not disabled. You can use the **no** form of this command to reset some of the logging criteria to their defaults. If you do not specify either option, all the logging types are reset to log on when the ARP packets are denied. The two options that are available are as follows:

- **acl-match**—Logging on ACL matches is reset to log on deny
- **dhcp-bindings**—Logging on DHCP bindings is reset to log on deny

**Examples**

This example shows how to configure an ARP inspection on VLAN 1 to add packets to a log that matches the ACLs:

```
Router# config terminal
Enter configuration commands, one per line. End with CNTL/Z
Router(config)# ip arp inspection vlan 1 logging acl-match matchlog
Router(config)#
```

**Related Commands**

Command	Description
<a href="#">arp access-list</a>	Configures an ARP ACL for ARP inspection and QoS filtering and enters the ARP ACL configuration submode.
<a href="#">show ip arp inspection</a>	Displays the status of DAI for a specific range of VLANs.

# ip auth-proxy max-login-attempts

To limit the number of login attempts at a firewall interface, use the **ip auth-proxy max-login-attempts** command. To return to the default settings, use the **no** form of this command.

**ip auth-proxy max-login-attempts** *l-maxint*

**no ip auth-proxy max-login-attempts**

<b>Syntax Description</b>	<i>l-maxint</i>	Maximum number of login attempts: valid values are from 1 to 2147483647 attempts.
---------------------------	-----------------	---

<b>Defaults</b>	<i>l-maxint</i> is 5.
-----------------	-----------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	<p>This command is supported on the firewall interfaces only.</p> <p>The maximum login attempt functionality is independent of the watch-list feature. If you do not configure a watch list (using the <b>ip access-list hardware permit fragments</b> command) and you configure a maximum login attempt, the existing authentication proxy behavior occurs but displays the new number for retries. If you configure a watch list, the IP address is put in the watch list, once the configured number of attempts has been reached.</p>
-------------------------	--

<b>Examples</b>	This example shows how to set a limit to the number of login attempts at a firewall interface:
-----------------	--

```
Router(config-if)# ip auth-proxy max-login-attempts 4
Router(config-if)#
```

Related Commands	Command	Description
	<b>clear ip auth-proxy watch-list</b>	Deletes a single watch-list entry or all watch-list entries.
	<b>ip auth-proxy watch-list</b>	Enables and configures an authentication proxy watch list.
	<b>show ip auth-proxy watch-list</b>	Displays the information about the authentication proxy watch list.

# ip auth-proxy watch-list

To enable and configure an authentication proxy watch list, use the **ip auth-proxy watch-list** command. See the “Usage Guidelines” section for the **no** form of this command usage.

```
ip auth-proxy watch-list [{add-item ip-addr} | enable | {expiry-time minutes}]
```

```
no ip auth-proxy watch-list [{add-item ip-addr} | expiry-time]
```

## Syntax Description

<b>add-item</b> <i>ip-addr</i>	Adds an IP address to the watch list.
<b>enable</b>	Enables a watch list.
<b>expiry-time</b> <i>minutes</i>	Specifies the duration of time that an entry is in the watch list; see the “Usage Guidelines” section for valid values.

## Defaults

The defaults are as follows:

- *minutes* is **30** minutes.
- The watch-list functionality is disabled.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

The valid values for minutes are from 0 to the largest 32-bit positive number (0x7FFFFFFF or 2147483647 in decimal). Setting the *minutes* to 0 (zero) places the entries in the list permanently.

This command is supported on the firewall interfaces only.

Use the **no** form of this command to do the following:

- **no ip auth-proxy watch-list**—Disables the watch-list functionality.
- **no ip auth-proxy watch-list add-item** *ip-addr*—Removes the IP address from the watch list.
- **no ip auth-proxy watch-list expiry-time**—Returns to the default setting.

A watch list consists of IP addresses that have opened TCP connections to port 80 and have not sent any data. No new connections are accepted from this type of IP address (to port 80) and the packet is dropped.

An entry remains in the watch list for the time that is specified by **expiry-time** *minutes*.

When you disable a watch list, no new entries are put into the watch list, but the sessions are put in SERVICE\_DENIED state. The timer deletes sessions after 2 minutes.

**Examples**

This example shows how to enable an authentication proxy watch list:

```
Router(config-if)# ip auth-proxy watch-list enable
Router(config-if)#
```

This example shows how to disable an authentication proxy watch list:

```
Router(config-if)# no ip auth-proxy watch-list
Router(config-if)#
```

This example shows how to add an IP address to a watch list:

```
Router(config-if)# ip auth-proxy watch-list add-item 12.0.0.2
Router(config-if)#
```

This example shows how to set the duration of time that an entry is in a watch list:

```
Router(config-if)# ip auth-proxy watch-list expiry-time 29
Router(config-if)#
```

**Related Commands**

Command	Description
<a href="#">clear ip auth-proxy watch-list</a>	Deletes a single watch-list entry or all watch-list entries.
<a href="#">ip auth-proxy max-login-attempts</a>	Limits the number of login attempts at a firewall interface.
<a href="#">show ip auth-proxy watch-list</a>	Displays the information about the authentication proxy watch list.

# ip casa

To configure the router to function as a forwarding agent, use the **ip casa** command. To disable the forwarding agent, use the **no** form of this command.

**ip casa** [*control-address* *igmp-address* [*udp-limit*]]

**no ip casa**

Syntax Description	
<i>control-address</i>	(Optional) IP address of the forwarding agent side of the services manager and forwarding agent tunnel used for sending signals.
<i>igmp-address</i>	IGMP address on which the forwarding agent will listen for wildcard and fixed affinities.
<i>udp-limit</i>	(Optional) Maximum UDP queue length; valid values are from 50 to 65535.

**Defaults** The default *udp-limit* value is 256.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** If more than the maximum *udp-limit* value arrives in a burst, the CASA wildcard updates from the service manager might get dropped.

The *control-address* value is unique for each forwarding agent.

**Examples** This example shows how to specify the IP address (10.10.4.1) and IGMP address (224.0.1.2) for the forwarding agent and set the UDP queue length to 300:

```
Router(config)# ip-casa 10.10.4.1 224.0.1.2 300
Router(config)#
```

Related Commands	Command	Description
	<b>forwarding-agent</b>	Specifies the port on which the forwarding agent listens for the wildcard and the fixed affinities.

## ip cef load-sharing algorithm

To select a CEF load-balancing algorithm, use the **ip cef load-sharing algorithm** command. To return to the default universal load-balancing algorithm, use the **no** form of this command.

**ip cef load-sharing algorithm** { **original** | **tunnel** [*id*] | **universal** [*id*]}

**no ip cef load-sharing algorithm** { **original** | **tunnel** [*id*] | **universal** [*id*]}

Syntax Description		
<b>original</b>	Sets the load-balancing algorithm to the original based on a source and destination hash.	
<b>tunnel</b>	Sets the load-balancing algorithm for use in tunnel environments or in environments where there are only a few IP source and destination address pairs.	
<b>universal</b>	Sets the load-balancing algorithm to the universal algorithm that uses a source, destination, and ID hash.	
<i>id</i>	(Optional) Fixed identifier.	

**Defaults** The universal load-balancing is selected.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The original CEF load-sharing algorithm produced distortions in load-balancing across multiple routers due to the use of the same algorithm on every router. When the load-balancing algorithm is set to universal mode, each router on the network can make a different load-balancing decision for each source-destination address pair which resolves load-balancing distortions.

Use the tunnel algorithm to share the load more fairly when only a few source-destination pairs are involved.

**Examples** This example shows how to enable the CEF load-balancing algorithm for universal environments:

```
Router(config)# ip cef load-sharing algorithm universal 1
Router(config)#
```

Related Commands	Command	Description
	<b>ip load-sharing</b>	Enables load balancing.

# ip cef table consistency-check

To enable the CEF-table consistency-checker types and parameters, use the **ip cef table consistency-check** command. To disable consistency checkers, use the **no** form of this command.

```
ip cef table consistency-check [type {lc-detect | scan-lc | scan-rib | scan-rp}] [count
count-number] [period seconds]
```

```
ip cef table consistency-check [settle-time seconds]
```

```
no ip cef table consistency-check [type {lc-detect | scan-lc | scan-rib | scan-rp}] [count
count-number] [period seconds]
```

```
no ip cef table consistency-check [settle-time seconds]
```

Syntax Description	type	(Optional) Specifies the type of consistency check to configure.
	<b>lc-detect</b>	(Optional) Specifies that the module detects a missing prefix.
	<b>scan-lc</b>	(Optional) Specifies a passive scan check of tables on the module.
	<b>scan-rib</b>	(Optional) Specifies a passive scan check of tables on the rendezvous point against RIB.
	<b>scan-rp</b>	(Optional) Specifies a passive scan check of tables on the rendezvous point.
	<b>count</b> <i>count-number</i>	(Optional) Specifies the maximum number of prefixes to check per scan; valid values are from 1 to 225.
	<b>period</b> <i>seconds</i>	(Optional) Specifies the period between scans; valid values are from 30 to 3600 seconds.
	<b>settle-time</b> <i>seconds</i>	(Optional) Specifies the time that elapsed during which updates for a candidate prefix are ignored as inconsistencies; valid values are from 1 to 3600 seconds.

**Defaults** Enabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

This command configures CEF-table consistency checkers and parameters for the detection mechanism types that are listed in [Table 2-12](#).

*Table 2-12 Detection Mechanism Types*

Mechanism	Operates On	Description
<b>Lc-detect</b>	Module	Operates on the module by retrieving IP prefixes found missing from its FIB table. If IP prefixes are missing, the module cannot forward packets for these addresses. Lc-detect sends IP prefixes to the rendezvous point for confirmation. If the rendezvous point detects that it has the relevant entry, an inconsistency is detected and a system message is displayed. Also, the rendezvous point sends a signal back to the module confirming that the IP prefix is an inconsistency.
<b>Scan-lc</b>	Module	Operates on the module by looking through the FIB table for a configurable time period and sending the next n prefixes to the rendezvous point. The rendezvous point does an exact lookup. If it finds the prefix missing, the rendezvous point reports an inconsistency. Finally, the rendezvous point sends a signal back to the module for confirmation.
<b>Scan-rp</b>	Route Processor	Operates on the rendezvous point (opposite of the scan-lc) by looking through the FIB table for a configurable time period and sending the next n prefixes to the module. The module does an exact lookup. If it finds the prefix missing, the module reports an inconsistency and finally signals the rendezvous point for confirmation.
<b>Scan-rib</b>	Route Processor	Operates on all RPs (even nondistributed) and scans the RIB to ensure that prefix entries are present in the rendezvous point FIB table.

**Examples**

This example shows how to enable the CEF-table consistency checkers:

```
Router(config)# ip cef table consistency-check
Router(config)#
```

**Related Commands**

Command	Description
<a href="#">clear ip cef inconsistency</a>	Clears the statistics and records for the CEF-consistency checker.
<a href="#">show ip cef inconsistency</a>	Displays the IP CEF inconsistencies.

# ip dhcp relay information option trust-all

To enable all the interfaces as trusted sources of the DHCP relay-agent information option, use the **ip dhcp relay information option trust-all** command. To return to the default settings, use the **no** form of this command.

**ip dhcp relay information option trust-all**

**no ip dhcp relay information option trust-all**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The DHCP server does not insert relay information.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

This command is used by cable access router termination systems. This functionality enables a DHCP server to identify the user (cable access router) sending the request and initiate appropriate action that is based on this information.

## Examples

This example shows how to specify that all interfaces on the router are trusted:

```
Router(config)# ip dhcp relay information option trust-all
Router(config)#
```

## Related Commands

Command	Description
<a href="#">show ip dhcp relay information trusted-sources</a>	Lists all the configured trusted interfaces.

# ip dhcp relay information trust

To enable an interface as a trusted source of the DHCP relay-agent information, use the **ip dhcp relay information trust** command. To return to the default settings, use the **no** form of this command.

**ip dhcp relay information trust**

**no ip dhcp relay information trust**

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

**Defaults** All interfaces on the router are untrusted.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Configuring an interface as a trusted source of relay-agent information allows the interface to receive DHCP discover or request packets. DHCP discover or request packets contain the relay-agent information option.

**Examples** This example shows how to specify that the interface is trusted:

```
Router(config)# ip dhcp relay information trust
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show ip dhcp relay information trusted-sources</a>	Lists all the configured trusted interfaces.

# ip dhcp route connected

To specify routes as connected routes, use the **ip dhcp route connected** command. To return to the default settings, use the **no** form of this command.

**ip dhcp route connected**

**no ip dhcp route connected**

---

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

---

**Defaults** All interfaces on the router are untrusted.

---

**Command Modes** Global configuration

---

Release	Modification
12.2(18)ZY	Support for this command was introduced.

---

---

**Usage Guidelines** If you enable the **ip dhcp route connected** command, DHCP downloads the route database from a database agent and adds the routes as connected routes, even though they may have been added as static routes previously.

---

**Examples** This example shows how to specify routes as connected routes:

```
Router(config)# ip dhcp route connected
Router(config)#
```

# ip dhcp snooping

To globally enable DHCP snooping, 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** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Wireless clients, or mobile nodes, gain access to an untrusted wireless network only if there is a corresponding entry in the DHCP snooping database. Enable DHCP snooping globally by entering the **ip dhcp snooping** command, and enable DHCP snooping on the tunnel interface by entering the **ip dhcp snooping packets** command. After you enable DHCP snooping, the process snoops DHCP packets to and from the mobile nodes and populates the DHCP snooping database.

**Examples** This example shows how to enable DHCP snooping:

```
Router(config) # ip dhcp snooping
Router(config) #
```

This example shows how to disable DHCP snooping:

```
Router(config) # no ip dhcp snooping
Router(config) #
```

Related Commands	Command	Description
	<b>ip dhcp snooping packets</b>	Enables DHCP snooping on the tunnel interface.
	<b>show ip dhcp snooping</b>	Displays the DHCP snooping configuration.
	<b>show ip dhcp snooping binding</b>	Displays the DHCP snooping binding entries.
	<b>show ip dhcp snooping database</b>	Displays the status of the DHCP snooping database agent.

## 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
interface-number } { expiry seconds }
```

```
no ip dhcp snooping binding mac-address vlan vlan-# ip-address interface interface
```

### Syntax Description

<i>mac-address</i>	MAC address.
<b>vlan</b> <i>vlan</i>	Specifies a valid VLAN number; valid values are from 1 to 4094.
<i>ip-address</i>	IP address.
<b>interface</b> <i>interface</i>	Specifies the interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> .
<i>interface-number</i>	Module and port number.
<b>expiry</b> <i>seconds</i>	Specifies the interval after which binding is no longer valid; valid values are from 1 to 4294967295 seconds.

### Defaults

This command has no default settings.

### Command Modes

Privileged EXEC

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

When you add or remove a binding using this command, the binding database is marked as changed and a write is initiated.

A maximum of 512 bindings are allowed in the DHCP snooping database.

### Examples

This example shows how to generate a DHCP binding configuration on interface gigabitethernet1/1 in VLAN 1 with an expiration time of 1000 seconds:

```
Router# ip dhcp snooping binding 0000.0c00.40af vlan 1 10.42.0.6 interface gi1/1 expiry 1000
Router#
```

Related Commands	Command	Description
	<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.
	<a href="#">show ip dhcp snooping binding</a>	Displays the DHCP snooping binding entries.
	<a href="#">show ip dhcp snooping database</a>	Displays the status of the DHCP snooping database agent.

# ip dhcp snooping database

To configure the DHCP-snooping database, use the **ip dhcp snooping database** command.

```
ip dhcp snooping database { bootflash:url | ftp:url | rtp:url | scp:url | sup-bootflash: | tftp:url }
```

```
ip dhcp snooping database { timeout timeout | write-delay time }
```

Syntax Description		
<b>bootflash:url</b>		Specifies the database URL for storing entries using the bootflash.
<b>ftp:url</b>		Specifies the database URL for storing entries using FTP.
<b>rtp:url</b>		Specifies the database URL for storing entries using RCP.
<b>scp:url</b>		Specifies the database URL for storing entries using SCP.
<b>sup-bootflash:</b>		Specifies the database URL for storing entries using the supervisor engine bootflash.
<b>tftp:url</b>		Specifies the database URL for storing entries using TFTP.
<b>timeout</b> <i>timeout</i>		Specifies the abort timeout interval; valid values are from 0 to 86400 seconds.
<b>write-delay</b> <i>time</i>		Specifies the amount of time before writing the DHCP-snooping entries to an external server after a change is seen in the local DHCP-snooping database; valid values are from 15 to 86400 seconds.

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

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** You must enable DHCP snooping on the interface before entering this command. Use the **ip dhcp snooping** command to enable DHCP snooping.

**Examples** This example shows how to specify the database URL using TFTP:

```
Router(config)# ip dhcp snooping database tftp://90.90.90.90/snooping-rp2
Router(config)#
```

This example shows how to specify the amount of time before writing DHCP snooping entries to an external server:

```
Router(config)# ip dhcp snooping database write-delay 15
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.
	<a href="#">show ip dhcp snooping binding</a>	Displays the DHCP snooping binding entries.
	<a href="#">show ip dhcp snooping database</a>	Displays the status of the DHCP snooping database agent.

# 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 [allow-untrusted]**

**no ip dhcp snooping information option**

<b>Syntax Description</b>	<b>allow-untrusted</b> (Optional) Enables the switch to accept incoming DHCP snooping packets with option 82 information from the edge switch.
---------------------------	--

<b>Defaults</b>	The defaults are as follows: <ul style="list-style-type: none"> <li>• <b>ip dhcp snooping information option</b>—Enabled</li> <li>• <b>ip dhcp snooping information option allow-untrusted</b>—Disabled</li> </ul>
-----------------	--

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	<p>DHCP option 82 is part of RFC 3046. DHCP is an application-layer protocol that is used for the dynamic configuration of TCP/IP networks. The protocol allows for a relay agent to pass DHCP messages between the DHCP clients and DHCP servers. By using a relay agent, servers do not have to be on the same network as the clients. Option 82 (82 is the option's code) addresses the security and scalability issues. Option 82 resides in the relay agent when DHCP packets that originate from the forwarding client are sent to the server. Servers that recognize option 82 may use the information to implement the IP address or other parameter assignment policies. The DHCP server echoes the option back to the relay agent in its replies. The relay agent strips out the option from the relay agent before forwarding the reply to the client.</p>
-------------------------	---

When you enter the **ip dhcp snooping information option allow-untrusted** on an aggregation switch that is connected to an edge switch through an untrusted interface, the aggregation switch accepts packets with option 82 information from the edge switch. The aggregation switch learns the bindings for hosts connected through an untrusted switch interface. You can enable the DHCP security features, such as dynamic ARP inspection or IP source guard, on the aggregation switch while the switch receives packets with option 82 information on untrusted input interfaces to which hosts are connected. You must configure the port on the edge switch that connects to the aggregation switch as a trusted interface.



### Caution

Do not enter the **ip dhcp snooping information option allow-untrusted** command on an aggregation switch that is connected to an untrusted device. If you enter this command, an untrusted device might spoof the option 82 information.

**Examples**

This example shows how to enable DHCP option 82 data insertion:

```
Router(config)# ip dhcp snooping information option
Router(config)#
```

This example shows how to disable DHCP option 82 data insertion:

```
Router(config)# no ip dhcp snooping information option
Router(config)#
```

This example shows how to enable the switch to accept incoming DHCP snooping packets with option 82 information from the edge switch:

```
Router(config)# ip dhcp snooping information option allow-trusted
Router(config)#
```

**Related Commands**

Command	Description
<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.
<a href="#">show ip dhcp snooping binding</a>	Displays the DHCP snooping binding entries.
<a href="#">show ip dhcp snooping database</a>	Displays the status of the DHCP snooping database agent.

# 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 message rate limiting, use the **no** form of this command.

**ip dhcp snooping limit rate** *rate*

**no ip dhcp snooping limit rate**

Syntax Description	<i>rate</i>
	Number of DHCP messages that a switch can receive per second; valid values are from 1 to 4294967294 seconds.

Defaults	Disabled
----------	----------

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Usage Guidelines	<p>This command is supported on Layer 2 switch-port and port-channel interfaces only.</p> <p>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.</p>
------------------	--

Examples	This example shows how to specify the number of DHCP messages that a switch can receive per second:
----------	---

```
Router(config-if)# ip dhcp snooping limit rate 150
Router(config)#
```

This example shows how to disable the DHCP message rate limiting:

```
Router(config-if)# no ip dhcp snooping limit rate
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.
	<a href="#">show ip dhcp snooping binding</a>	Displays the DHCP snooping binding entries.
	<a href="#">show ip dhcp snooping database</a>	Displays the status of the DHCP snooping database agent.

# ip dhcp snooping packets

To enable DHCP snooping on the tunnel interface, use the **ip dhcp snooping packets** command. To disable DHCP snooping, use the **no** form of this command.

**ip dhcp snooping packets**

**no ip dhcp snooping packets**

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

**Defaults** Disabled

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command is supported on Layer 2 switch-port and port-channel interfaces only. This command is supported on Catalyst 6500 series switches that are configured with a WLSM only. Wireless clients, or mobile nodes, gain access to an untrusted wireless network only if there is a corresponding entry in the DHCP snooping database. Enable DHCP snooping globally by entering the **ip dhcp snooping** command, and enable DHCP snooping on the tunnel interface by entering the **ip dhcp snooping packets** command. After you enable DHCP snooping, the process snoops DHCP packets to and from the mobile nodes and populates the DHCP snooping database.

**Examples** This example shows how to enable DHCP snooping:

```
Router(config)# ip dhcp snooping packets
Router(config)#
```

This example shows how to disable DHCP snooping:

```
Router(config)# no ip dhcp snooping packets
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.
	<a href="#">show ip dhcp snooping binding</a>	Displays the DHCP snooping binding entries.
	<a href="#">show ip dhcp snooping database</a>	Displays the status of the DHCP snooping database agent.

# ip dhcp snooping verify mac-address

To verify that the source MAC address in a DHCP packet matches the client hardware address on an untrusted port, use the **ip dhcp snooping verify mac-address** command. To disable verification, use the **no** form of this command.

**ip dhcp snooping verify mac-address**

**no ip dhcp snooping verify mac-address**

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

**Defaults** Enabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** For untrusted DHCP snooping ports, DHCP snooping verifies the MAC address on the client hardware address field to ensure that a client is requesting multiple addresses from a single MAC address. You can use the **ip dhcp snooping verify mac-address** command to trust the ports or you can use the **no ip dhcp snooping verify mac-address** command to leave the ports untrusted by disabling the MAC address verification on the client hardware address field.

**Examples** This example shows how to verify that the source MAC address in a DHCP packet matches the client hardware address on an untrusted port:

```
Router(config)# ip dhcp snooping verify mac-address
Router(config)#
```

This example shows how to turn off the verification of the MAC address on the client hardware address field:

```
Router(config)# no ip dhcp snooping verify mac-address
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.
	<a href="#">show ip dhcp snooping binding</a>	Displays the DHCP snooping binding entries.
	<a href="#">show ip dhcp snooping database</a>	Displays the status of the DHCP snooping database agent.

# ip dhcp snooping vlan

To enable DHCP snooping on a VLAN or a group of VLANs, use the **ip dhcp snooping vlan** command. To disable DHCP snooping on a VLAN or a group of VLANs, use the **no** form of this command.

**ip dhcp snooping vlan** {*number* | *vlanlist*}

**no ip dhcp snooping vlan** {*number* | *vlanlist*}

<b>Syntax Description</b>	<i>number</i>   <i>vlanlist</i>	VLAN number or a group of VLANs; valid values are from 1 to 4094. See the “Usage Guidelines” section for additional information.
<b>Defaults</b>	Disabled	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.
<b>Usage Guidelines</b>	<p>DHCP snooping is enabled on a VLAN only if both the global snooping and the VLAN snooping are enabled.</p> <p>Enter the range of VLANs using this format: 1,3-5,7,9-11.</p>	
<b>Examples</b>	<p>This example shows how to enable DHCP snooping on a VLAN:</p> <pre>Router(config)# ip dhcp snooping vlan 10 Router(config)#</pre> <p>This example shows how to disable DHCP snooping on a VLAN:</p> <pre>Router(config)# no ip dhcp snooping vlan 10 Router(config)#</pre> <p>This example shows how to enable DHCP snooping on a group of VLANs:</p> <pre>Router(config)# ip dhcp snooping vlan 10,4-8,55 Router(config)#</pre> <p>This example shows how to disable DHCP snooping on a group of VLANs:</p> <pre>Router(config)# no ip dhcp snooping vlan 10,4-8,55 Router(config)#</pre>	

Related Commands	Command	Description
	<b>show ip dhcp snooping</b>	Displays the DHCP snooping configuration.
	<b>show ip dhcp snooping binding</b>	Displays the DHCP snooping binding entries.
	<b>show ip dhcp snooping database</b>	Displays the status of the DHCP snooping database agent.

# ip flow-aggregation cache

To create a flow-aggregation cache and enter the aggregation cache configuration mode, use the **ip flow-aggregation cache** command. To negate a command or return to its default settings, use the **no** form of this command.

**ip flow-aggregation cache** { **as** | **destination-prefix** | **prefix** | **protocol-port** | **source-prefix** }

**no ip flow-aggregation cache** { **as** | **destination-prefix** | **prefix** | **protocol-port** | **source-prefix** }

## Syntax Description

<b>as</b>	Configures the autonomous-system aggregation-cache scheme.
<b>destination-prefix</b>	Configures the destination-prefix aggregation-cache scheme.
<b>prefix</b>	Configures the prefix aggregation-cache scheme.
<b>protocol-port</b>	Configures the protocol-port aggregation-cache scheme.
<b>source-prefix</b>	Configures the source-prefix aggregation-cache scheme.

## Defaults

The defaults are as follows:

- **entries** *num* is 4096 entries.
- **active** *time* is 30 minutes.
- **inactive** *time* is 15 seconds.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

In source-prefix aggregation mode, only the source mask is configurable. In destination-prefix aggregation mode, only the destination mask is configurable.

Once you enter the flow aggregation cache configuration mode, these commands are available:

- **cache** { **entries** *num* } | { **timeout** { **active** *time* } | { **inactive** *time* } }
- **default** { **cache** { **entries** | **timeout** } } | **enabled** | { **export destination** }
- **enabled**
- **export destination** *ip-addr udp-port-num*

The syntax descriptions are as follows:

<b>cache</b>	Configures the NetFlow cache parameters.
<b>entries</b> <i>num</i>	Specifies the number of entries in the flow cache; valid values are from 1024 to 524288 flow entries.
<b>timeout</b>	Specifies the timeout parameters for the flow cache.
<b>active</b> <i>time</i>	Specifies the active flow timeout; valid values are from 1 to 60 minutes.
<b>inactive</b> <i>time</i>	Specifies the inactive flow timeout; valid values are from 10 to 600 seconds.
<b>default</b>	Sets a command to its default.
<b>enabled</b>	Enables the aggregation cache.
<b>export destination</b>	Specifies the host or port to send flow statistics.
<i>ip-addr</i>	Destination IP address or hostname.
<i>udp-port-num</i>	UDP port number; valid values are from 1 to 65535.

### Examples

This example shows how to enable an autonomous-system aggregation-cache scheme:

```
Router(config)# ip flow-aggregation cache as
Router(config-flow-cache)# enable
Router(config-flow-cache)#
```

### Related Commands

Command	Description
<a href="#">show ip cache flow</a>	Displays a summary of the NetFlow cache-flow entries.

## ip flow-cache entries

To change the number of entries that are maintained in the NetFlow cache, use the **ip flow-cache entries** command. To return to the default number of entries, use the **no** form of this command.

**ip flow-cache entries** *number*

**no ip flow-cache entries**

<b>Syntax Description</b>	<i>number</i>	Number of entries to maintain in the NetFlow cache; valid values are from 1024 to 524288 entries.
<b>Defaults</b>	65536 entries	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

Typically, the default size of the NetFlow cache will meet your needs. However, you can increase or decrease the number of entries that are maintained in the cache to meet the needs of your flow traffic rates. For environments with a high amount of flow traffic (such as an Internet core router), we recommend that you maintain a larger value such as 131072. To obtain information on your flow traffic, use the **show ip cache flow** command.

Each cache entry is approximately 64 bytes of storage. Assuming a cache with the default number of entries, approximately 4 MB of DRAM would be required. Each time that a new flow is taken from the free-flow queue, the number of free flows is checked. If there are only a few free flows remaining, NetFlow attempts to age 30 flows using an accelerated timeout. If there is only one free flow remaining, NetFlow automatically ages 30 flows regardless of their age. This action ensures that free flow entries are always available.



### Caution

We recommend that you do not change the number of entries in the NetFlow cache. Improper use of this feature could cause network problems. To return to the default number of entries in the NetFlow cache, use the **no ip flow-cache entries** command.

---

**Examples**

This example shows how to increase the number of entries in the NetFlow cache to 131072:

```
Router(config)# ip flow-cache entries 131072
Router(config)# exit
```

---

**Related Commands**

Command	Description
<a href="#">show ip cache flow</a>	Displays a summary of the NetFlow cache-flow entries.

---

# ip flow-export

To globally enable NDE for the hardware-switched flows, use the **ip flow-export** command. To disable NDE for the hardware-switched flows, use the **no** form of this command.

**ip flow-export**

**no ip flow-export**

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

**Defaults** The defaults are as follows:

- Disabled
- Version 7

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** To change the default NDE version, use the **ip flow-export hardware version** command.

**Examples** This example shows how to enable NDE for the hardware-switched flows:

```
Router(config)# ip flow-export
Router(config)#
```

This example shows how to disable NDE for the hardware-switched flows:

```
Router(config)# no ip flow-export
Router(config)#
```

Related Commands	Command	Description
	<b>ip flow-export hardware version</b>	Specifies the NDE version for hardware-switched flows.
	<b>show mls nde</b>	Displays information about the NDE hardware-switched flow.

## ip flow-export destination

To export the NetFlow cache entries to a specific destination, use the **ip flow-export destination** command. To disable information exporting, use the **no** form of this command.

**ip flow-export destination** {*hostname* | *ip-address*} *udp-port*

**no ip flow-export destination**

Syntax Description		
	<i>hostname</i>	IP hostname of the workstation to which you want to export the NetFlow information.
	<i>ip-address</i>	IP address of the workstation to which you want to export the NetFlow information.
	<i>udp-port</i>	UDP protocol-specific port number.

**Defaults** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** You can enter two destination IP addresses to improve the probability of receiving complete NetFlow data by providing redundant data streams.

To configure multiple NetFlow export destinations to a router, enter the **ip flow-export destination** command twice, once for each destination. Do not enter the same IP address twice. However, entering two different IP addresses with the same UDP port number is configurable.

A NetFlow cache entry contains a lot of information. When flow switching is enabled with the **ip route-cache flow** command, you can use the **ip flow-export destination** command to configure the router to export the flow cache entry to a workstation when a flow expires. This feature can be useful for statistics, billing, and security, for example.

When entering the *ip-address* value, follow these guidelines:

- You cannot enter the IP address of the interface that you are currently on; you must use an address from the subnet of any interface that is not being used.
- You cannot use an address from a loopback interface; loopback interfaces do not have internal VLAN IDs or MAC addresses.

To specify the source IP address of the data, use the **ip flow-export source** command. To specify the version that is used on the workstation that receives the NetFlow data, use the **ip flow-export version** command.

For more information on NDE, refer to the “Configuring NDE” chapter in the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*.

## ip flow-export destination

### Examples

This example shows how to export a NetFlow cache entry to UDP port 125 using the version 1 format on the workstation that has an IP address of 10.42.42.1 99917:

```
Router# configure terminal
Router(config)# ip flow-export destination 10.42.42.1 9991 125
Router(config)# exit
```

### Related Commands

Command	Description
<a href="#">ip flow-export source</a>	Specifies the source interface IP address that is used in the NDE datagram.
<a href="#">ip flow-export version</a>	Specifies the version for the export of information in NetFlow cache entries.
<a href="#">ip route-cache flow</a>	Enables NetFlow switching for IP routing.

# ip flow-export hardware version

To specify the NDE version for hardware-switched flows, use the **ip flow-export hardware version** command. To return to the default settings, use the **no** form of this command.

**ip flow-export hardware version** [5 | 7]

**no ip flow-export hardware version**

Syntax Description		
	<b>5</b>	Specifies that the export packet uses the version 5 format; see the “Usage Guidelines” section for additional information.
	<b>7</b>	Specifies that the export packet uses the version 7 format; see the “Usage Guidelines” section for additional information.

**Defaults** Version 7

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to specify the NDE version for hardware-switched flows:

```
Router(config)# ip flow-export hardware version 5
Router(config)#
```

Related Commands	Command	Description
	<a href="#">ip flow-export interface</a>	Enables the interface-based ingress NDE for hardware-switched flows.
	<a href="#">show mls nde</a>	Displays information about the NDE hardware-switched flow.

# ip flow-export interface

To enable the interface-based ingress NDE for hardware-switched flows, use the **ip flow-export interface** command. To disable interface-based NDE for hardware-switched flows, use the **no** form of this command.

**ip flow-export interface**

**no ip flow-export interface**

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

**Defaults** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Use the **ip flow-export interface** command with the **ip flow ingress** command to enable or disable NDE on a specific interface.

**Examples** This example shows how to enable interface-based NDE for hardware-switched flows:

```
Router(config)# ip flow-export interface
Router(config)#
```

This example shows how to disable interface-based NDE for hardware-switched flows:

```
Router(config)# no ip flow-export interface
Router(config)#
```

Related Commands	Command	Description
	<b>ip flow-export hardware version</b>	Specifies the NDE version for hardware-switched flows.
	<b>show ip flow-export</b>	Displays the information about the hardware-switched and software-switched flows for the data export, including the main cache and all other enabled caches.
	<b>show mls nde</b>	Displays information about the NDE hardware-switched flow.

## ip flow-export source

To specify the source interface IP address that is used in the NDE datagram, use the **ip flow-export source** command. To remove the source address, use the **no** form of this command.

**ip flow-export source** [{*interface interface-number*} | {**null** *interface-number*} | {**port-channel** *number*} | {**vlan** *vlan-id*}]

**no ip flow-export source** [{*interface interface-number*} | {**null** *interface-number*} | {**port-channel** *number*} | {**vlan** *vlan-id*}]

Syntax Description	
<i>interface</i>	(Optional) Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , <b>ge-wan</b> , and <b>atm</b> .
<i>interface-number</i>	(Optional) Module and port number; see the “Usage Guidelines” section for valid values.
<b>null</b> <i>interface-number</i>	(Optional) Specifies the null interface; the valid value is <b>0</b> .
<b>port-channel</b> <i>number</i>	(Optional) Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 256.
<b>vlan</b> <i>vlan-id</i>	(Optional) Specifies the VLAN; valid values are from 1 to 4094.

**Defaults** No source interface is specified.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

After you configure NDE, you can specify the source interface that is used in the UDP datagram containing the export data. The NetFlow Collector on the workstation uses the IP address of the source interface to determine which router sent the information. The NetFlow Collector performs SNMP queries to the router using the IP address of the source interface. Because the IP address of the source interface can change (for example, the interface might flap so a different interface is used to send the data), we recommend that you configure a loopback source interface. A loopback interface is always up and can respond to SNMP queries from the NetFlow Collector on the workstation.

For more information on NDE, refer to the “Configuring NDE” chapter in the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*.

### Examples

This example shows the configuration for a loopback source interface. The loopback interface has the IP address as 4.0.0.1 and is used by the serial interface in slot 5, port 0:

```
Router# configure terminal
Router(config)# interface loopback0
Router(config-if)# ip address 4.0.0.1 255.0.0.0
Router(config-if)# exit
Router(config)# interface serial 5/0:0
Router(config-if)# ip unnumbered loopback0
Router(config-if)# no ip mroute-cache
Router(config-if)# encapsulation ppp
Router(config-if)# ip route-cache flow
Router(config-if)# exit
Router(config)# ip flow-export source loopback0
Router(config)# exit
```

### Related Commands

Command	Description
<a href="#">ip flow-export destination</a>	Exports the NetFlow cache entries to a specific destination.
<a href="#">ip flow-export version</a>	Specifies the version for the export of information in NetFlow cache entries.
<a href="#">ip route-cache flow</a>	Enables NetFlow switching for IP routing.

## ip flow-export version

To specify the version for the export of information in NetFlow cache entries, use the **ip flow-export version** command. To return to the default settings, use the **no** form of this command.

```
ip flow-export version { 1 | { 5 [origin-as | peer-as] } | { 9 [bgp-nexthop | origin-as | peer-as] } }
no ip flow-export version
```

Syntax Description		
	<b>1</b>	Specifies that the export packet use the version 1 format; see the “Usage Guidelines” section for additional information.
	<b>5</b>	Specifies that the export packet use the version 5 format; see the “Usage Guidelines” section for additional information.
	<b>origin-as</b>	(Optional) Specifies that export statistics include the origin autonomous system for the source and destination.
	<b>peer-as</b>	(Optional) Specifies that export statistics include the peer autonomous system for the source and destination.
	<b>9</b>	Specifies that the export packet uses the version 9 format; see the “Usage Guidelines” section for additional information.
	<b>bgp-nexthop</b>	(Optional) Specifies that export statistics include the BGP next hop for the source and destination.

**Defaults** Export of information in NetFlow cache entries is disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Version 5 and version 9 formats include the source and destination autonomous-system addresses and source and destination prefix masks. Also, version 9 includes BGP next-hop information.

The number of records stored in the datagram is a variable from 1 to 24 for version 1. The number of records stored in the datagram is a variable between 1 and 30 for version 5.

For more information on NDE, refer to the “Configuring NDE” chapter in the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*.

**ip flow-export version****Examples**

This example shows how to export the data using the version 5 format:

```
Router(config)# ip flow-export version 5
Router(config)#
```

**Related Commands**

Command	Description
<a href="#">show mls nde</a>	Displays information about the NDE hardware-switched flow.

# ip flow ingress

To enable the software-switched flow creation in Layer 3, use the **ip flow ingress** command. To return to the default settings, use the **no** form of this command.

**ip flow ingress**

**no ip flow ingress**

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

**Defaults** Disabled

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** To create a NetFlow entry, you need to enter the **ip flow ingress** command.

Follow these guidelines to display multicast entries:

- Enter the **show mls netflow ip** command.
- Enter the **ip flow ingress** command on an interface.
- Make sure that you have not entered the **no ip multicast netflow ingress** command.

**Examples** This example shows how to enable inbound NDE for IPv4-bridged flows and NetFlow entry creation:

```
Router(config-if)# ip flow ingress
Router(config-if)#
```

This example shows how to disable inbound NDE for IPv4-bridged flows:

```
Router(config-if)# no ip flow ingress
Router(config-if)#
```

# ip flow layer2-switched

To enable the creation of switched, bridged, and Layer 2 IP flows for a specific VLAN, use the **ip flow layer2-switched** command. To return to the default settings, use the **no** form of this command.

```
ip flow { ingress | export } layer2-switched { vlan { num / vlanlist } }
```

```
no ip flow { ingress | export } layer2-switched { vlan { num / vlanlist } }
```

Syntax Description		
<b>ingress</b>		Enables the collection of switched, bridged, and IP flows in Layer 2.
<b>export</b>		Enables the export of switched, bridged, and IP flows in Layer 2.
<b>vlan</b> <i>num</i> / <i>vlanlist</i>		Specifies the VLAN or range of VLANs; valid values are from 1 to 4094. See the “Usage Guidelines” section for additional information.

## Defaults

The defaults are as follows:

- **ip flow ingress layer2switch** is disabled.
- **ip flow export layer2switched** is enabled.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

Before using this command, you must ensure that a corresponding VLAN interface is available and has a valid IP address.

You can enter one or multiple VLANs. The following examples are samples of valid VLAN lists: 1; 1,2,3; 1-3,7.

## Examples

This example shows how to enable the collection of Layer 2-switched flows on a specific VLAN:

```
Router(config)# ip flow ingress layer2-switched vlan 2
Router(config)#
```

This example shows how to enable export of Layer 2-switched flows on a range of VLANs:

```
Router(config)# ip flow export layer2-switched vlan 1-3,7
Router(config)#
```

This example shows how to disable the collection of Layer 2-switched flows on a specific VLAN:

```
Router(config)# no ip flow ingress layer2-switched vlan 2
Router(config)#
```

# ip forward-protocol turbo-flood

To speed up the flooding of UDP packets using the spanning-tree algorithm, use the **ip forward-protocol turbo-flood** command. To return to the default settings, use the **no** form of this command.

**ip forward-protocol turbo-flood [udp-checksum]**

**no ip forward-protocol turbo-flood [udp-checksum]**

Syntax Description	<b>udp-checksum</b>	(Optional) Specifies the UDP checksum.
--------------------	---------------------	--

Defaults	Disabled
----------	----------

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Usage Guidelines	When you enter the <b>ip forward-protocol turbo-flood</b> command, the outgoing UDP packets have a NULL checksum. If you want to have UDP checksums on all outgoing packets, you must enter the <b>ip forward-protocol turbo-flood udp-checksum</b> command.
------------------	--

Examples	This example shows how to speed up the flooding of UDP packets using the spanning-tree algorithm:
----------	---

```
Router(config)# ip forward-protocol turbo-flood
Router(config)#
```

This example shows how to speed up the flooding of UDP packets using the spanning-tree algorithm and have the UDP checksums on all outgoing packets:

```
Router(config)# ip forward-protocol turbo-flood udp-checksum
Router(config)#
```

This example shows how to turn off the **udp-checksum** keyword and the **ip forward-protocol turbo-flood** command:

```
Router(config)# no ip forward-protocol turbo-flood udp-checksum
Router(config)#
```

This example shows how to reinstate the **ip forward-protocol turbo-flood** command without the **udp-checksum** keyword:

```
Router(config)# ip forward-protocol turbo-flood
Router(config)#
```

---

**Related Commands**

Command	Description
<b>ip forward-protocol</b>	Specifies that protocols and ports that the router forwards when forwarding broadcast packets.

## ip igmp immediate-leave group-list

To enable the immediate processing of the IGMP leave-group messages, use the **ip igmp immediate-leave group-list** command. To return to the default settings, use the **no** form of this command.

**ip igmp immediate-leave group-list** *acl*

**no ip igmp immediate-leave group-list** *acl*

<b>Syntax Description</b>	<i>acl</i>	Group ACL number; see the “Usage Guidelines” section for valid values.
<b>Defaults</b>	Disabled	
<b>Command Modes</b>	Global or interface configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.
<b>Usage Guidelines</b>	<p>If you enter the <b>ip igmp immediate-leave group-list</b> command, you must enter this command in VLAN interface configuration mode only.</p> <p>Valid values for the <i>acl</i> argument are as follows:</p> <ul style="list-style-type: none"> <li>• Access-list number—1 to 99</li> <li>• Expanded range access-list number—1300 to 1999</li> <li>• Name of the standard IP access list</li> </ul> <p>You can configure one or the other but not both configuration modes at the same time.</p> <p>You can enter the <i>acl</i> value to restrict the immediate-leave behavior to a simple access list for multicast groups. The IGMP leave-group messages for multicast groups that are not permitted by the <i>acl</i> value has the standard inquiry mechanism/leave latency.</p>	
<b>Examples</b>	<p>This example shows how to enable the immediate processing of the IGMP leave-group messages:</p> <pre>Router(config)# ip igmp immediate-leave group-list 3 Router(config)#</pre>	

# ip igmp last-member-query-interval

To configure the last-member query interval for the IGMP, use the **ip igmp last-member-query-interval** command. To return to the default settings, use the **no** form of this command.

**ip igmp last-member-query-interval** *interval*

**no ip igmp last-member-query-interval**

<b>Syntax Description</b>	<i>interval</i>	Interval for the last-member query; valid values are from 100 to 65535 milliseconds in multiples of 100 milliseconds.
---------------------------	-----------------	---

<b>Defaults</b>	1000 milliseconds (1 second); see the “Usage Guidelines” section for additional information.
-----------------	--

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

When a multicast host leaves a group, the host sends an IGMP leave. To check if this host is the last to leave the group, an IGMP query is sent out when the leave is seen and a timer is started. If no reports are received before the timer expires, the group record is deleted.

The *interval* is the actual time that the Catalyst 6500 series switch waits for a response for the group-specific query.

If you enter an interval that is not a multiple of 100, the interval is rounded to the next lowest multiple of 100. For example, if you enter 999, the interval is rounded down to 900 milliseconds.

If IGMP fast-leave processing is enabled and you enter the **no ip igmp last-member-query-interval** command, the interval is set to 0 seconds; immediate leave always assumes higher priority.

**Examples**

This example shows how to configure the last-member query interval to 200 milliseconds:

```
Router(config-if)# ip igmp last-member-query-interval 200
Router(config-if)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ip igmp immediate-leave group-list</b>	Enables the immediate processing of the IGMP leave-group messages.
	<b>show ip igmp interface</b>	Displays the information about the IGMP-interface status and configuration.



# 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**

**no ip igmp snooping**

---

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

---

**Defaults** The defaults are as follows:

- IGMP snooping is enabled on the Catalyst 6500 series switch.
- IGMP snooping is not configured on multicast routers.

---

**Command Modes** Interface configuration

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Usage Guidelines** Before you can enable IGMP snooping on the Catalyst 6500 series switches, you must configure the VLAN interface for multicast routing.

Enter this command in VLAN interface configuration mode only.

---

**Examples** This example shows how to enable IGMP snooping:

```
Router(config-if)# ip igmp snooping
Router(config-if)#
```

This example shows how to disable IGMP snooping:

```
Router(config-if)# no ip igmp snooping
Router(config-if)#
```

Related Commands	Command	Description
	<b>ip igmp snooping fast-leave</b>	Enables the IGMPv3-snooping fast-leave processing.
	<b>ip igmp snooping mrouter</b>	Configures a Layer 2 port as a multicast router port.
	<b>show ip igmp snooping explicit-tracking</b>	Displays the information about the explicit host-tracking status for IGMPv3 hosts.

## ip igmp snooping explicit-tracking

To enable explicit host tracking, use the **ip igmp snooping explicit-tracking** command. To disable the explicit host tracking, use the **no** form of this command.

**ip igmp snooping explicit-tracking**

**no ip igmp snooping explicit-tracking**

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

**Defaults** Enabled

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Explicit host tracking is supported only with IGMPv3 hosts.

When you enable explicit host tracking and the Catalyst 6500 series switch is working in proxy-reporting mode, the router may not be able to track all the hosts that are behind a VLAN interface. In proxy-reporting mode, the Catalyst 6500 series switch forwards only the first report for a channel to the router and suppresses all other reports for the same channel.

With IGMPv3 proxy reporting, the Catalyst 6500 series switch does proxy reporting for unsolicited reports and reports that are received in the general query interval.

Proxy reporting is turned on by default. When you disable proxy reporting, the Catalyst 6500 series switch works in transparent mode and updates the IGMP snooping database as it receives reports and forwards this information to the upstream router. The router can then explicitly track all reporting hosts.

Disabling explicit tracking disables fast-leave processing and proxy reporting.

IGMPv3 supports explicit host tracking of membership information on any port. The explicit host-tracking database is used for fast-leave processing for IGMPv3 hosts, proxy reporting, and statistics collection. When you enable explicit host tracking on a VLAN, the IGMP snooping software processes the IGMPv3 report that it receives from a host and builds an explicit host-tracking database that contains the following information:

- The port that is connected to the host.
- The channels that are reported by the host.
- The filter mode for each group that is reported by the host.
- The list of sources for each group that is reported by the hosts.
- The router filter mode of each group.
- For each group, the list of hosts that request the source.

---

**Examples**

This example shows how to enable IGMPv3-explicit host tracking:

```
Router(config-if)# ip igmp snooping explicit-tracking
Router(config-if)#
```

This example shows how to disable IGMPv3-explicit host tracking:

```
Router(config-if)# no ip igmp snooping explicit-tracking
Router(config-if)#
```

---

**Related Commands**

Command	Description
<a href="#">ip igmp snooping limit track</a>	Limits the size of the explicit-tracking database.
<a href="#">show ip igmp snooping explicit-tracking</a>	Displays the information about the explicit host-tracking status for IGMPv3 hosts.

# ip igmp snooping fast-leave

To enable the IGMPv3-snooping fast-leave processing, use the **ip igmp snooping fast-leave** command. To disable fast-leave processing, use the **no** form of this command.

**ip igmp snooping fast-leave**

**no ip igmp snooping fast-leave**

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

**Defaults** The defaults are as follows:

- IGMP version 2—Disabled
- IGMP version 3—Enabled

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Enter this command in VLAN interface configuration mode only.



**Note**

Fast-leave processing is enabled by default. To disable fast-leave processing, you must enter the **no ip igmp snooping fast-leave** command to disable fast-leave processing.

You should use the IGMPv3-snooping fast-leave processing when there is a single receiver for the MAC group for a specific VLAN.

**Examples** This example shows how to enable IGMPv3-snooping fast-leave processing:

```
Router(config-if)# ip igmp snooping fast-leave
Router(config-if)#
```

This example shows how to disable IGMPv3-snooping fast-leave processing:

```
Router(config-if)# no ip igmp snooping fast-leave
Router(config-if)#
```

Related Commands	Command	Description
	<a href="#">ip igmp snooping</a>	Enables IGMP snooping.
	<a href="#">ip igmp snooping explicit-tracking</a>	Enables explicit host tracking.
	<a href="#">show ip igmp interface</a>	Displays the information about the IGMP-interface status and configuration.
	<a href="#">show mac-address-table</a>	Displays the information about the MAC-address table.

## ip igmp snooping flooding

To configure periodic flooding of multicast packets, use the **ip igmp snooping flooding** command. To disable periodic flooding, use the **no** form of this command.

**ip igmp snooping flooding** [**timer** *seconds*]

**no ip igmp snooping flooding**

<b>Syntax Description</b>	<b>timer</b> <i>seconds</i>	(Optional) Specifies the interval between flooding in a 24-hour period for source-only entries; valid values are from 0 to 86400 seconds.
---------------------------	-----------------------------	---

<b>Defaults</b>	The defaults are as follows: <ul style="list-style-type: none"> <li>• Disabled.</li> <li>• If enabled, <i>seconds</i> is <b>600</b> seconds (10 minutes).</li> </ul>
-----------------	--

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

<b>Command History</b>	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	<p>This command is supported on source-only VLANs.</p> <p>You can enter <b>0</b> seconds to disable flooding. If you enter a maximum of 86400 seconds, flooding would occur once every 24 hours.</p>
-------------------------	--

<b>Examples</b>	<p>This example shows how to specify the interval between flooding in a 24-hour period:</p> <pre>Router(config-if)# ip igmp snooping flooding timer 300 Router(config-if)#</pre>
-----------------	--

# ip igmp snooping l2-entry-limit

To configure the maximum number of Layer 2 entries that can be created by the Catalyst 6500 series switch, use the **ip igmp snooping l2-entry-limit** command.

**ip igmp snooping l2-entry-limit** *max-entries*

Syntax Description	<i>max-entries</i>	Maximum number of Layer 2 entries that can be created by the Catalyst 6500 series switch; valid values are from 1 to 100000.
--------------------	--------------------	--

Defaults	15488 Layer 2 entries
----------	-----------------------

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Usage Guidelines	When entering <i>max-entries</i> , do not enter a comma (.).
	Enter this command in VLAN interface configuration mode only.

**Examples** This example shows how to configure the maximum number of Layer 2 entries that can be created by the Catalyst 6500 series switch:

```
Router(config-if)# ip igmp snooping l2-entry-limit 25000
Router(config-if)#
```

Related Commands	Command	Description
	<b>show ip igmp interface</b>	Displays the information about the IGMP-interface status and configuration.

## ip igmp snooping last-member-query-interval

To configure the last member query interval for IGMP snooping, use the **ip igmp snooping last-member-query-interval** command. To return to the default settings, use the **no** form of this command.

**ip igmp snooping last-member-query-interval** *interval*

**no ip igmp snooping last-member-query-interval**

<b>Syntax Description</b>	<i>interval</i>	Interval for the last member query; valid values are from 100 to 900 milliseconds in multiples of 100 milliseconds.
---------------------------	-----------------	---

<b>Defaults</b>	1000 milliseconds (1 second); see the “Usage Guidelines” section for additional information.
-----------------	--

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** When a multicast host leaves a group, the host sends an IGMP leave. To check if this host is the last to leave the group, an IGMP query is sent out when the leave is seen and a timer is started. If no reports are received before the timer expires, the group record is deleted.

The *interval* is the actual time that the Catalyst 6500 series switch waits for a response for the group-specific query.

If you enter an interval that is not a multiple of 100, the interval is rounded to the next lowest multiple of 100. For example, if you enter 999, the interval is rounded down to 900 milliseconds.

If you enable IGMP fast-leave processing and you enter the **no ip igmp snooping last-member-query-interval** command, the interval is set to 0 seconds; fast-leave processing always assumes higher priority.

Even though the valid interval range is 100 to 1000 milliseconds, you cannot enter a value of **1000**. If you want this value, you must enter the **no ip igmp snooping last-member-query-interval** command and return to the default value (1000 milliseconds).

---

**Examples**

This example shows how to configure the last-member-query-interval to 200 milliseconds:

```
Router(config-if)# ip igmp snooping last-member-query-interval 200
Router(config-if)#
```

---

**Related Commands**

Command	Description
<b>ip igmp snooping fast-leave</b>	Enables the IGMP v3-snooping fast-leave processing.
<b>show ip igmp interface</b>	Displays the information about the IGMP-interface status and configuration.

---

# ip igmp snooping limit track

To limit the size of the explicit-tracking database, use the **ip igmp snooping limit track** command. To return to the default settings, use the **no** form of this command.

**ip igmp snooping limit track** *max-entries*

**no ip igmp snooping limit track**

<b>Syntax Description</b>	<i>max-entries</i>	Maximum number of entries in the explicit-tracking database; valid values are from 0 to 128000 entries.
---------------------------	--------------------	---

<b>Defaults</b>	<i>max-entries</i> is <b>32000</b> .
-----------------	--------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	<p>Each entry in the explicit-tracking database is identified by the source IP, group IP, port, VLAN, and reporter IP.</p> <p>When you set the <i>max-entries</i> to <b>0</b>, explicit tracking is disabled.</p> <p>When the explicit-tracking database exceeds the configured <i>max-entries</i>, a syslog message is generated.</p> <p>When you reduce the <i>max-entries</i>, the explicit-tracking database does not decrease in size immediately. The explicit-tracking database gradually shrinks as reporters time out.</p>
-------------------------	---

<b>Examples</b>	<p>This example shows how to configure the maximum number of entries in the explicit-tracking database:</p> <pre>Router(config)# ip igmp snooping limit track 20000 Router(config)#</pre>
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">ip igmp snooping explicit-tracking</a>	Enables explicit host tracking.
	<a href="#">show ip igmp snooping explicit-tracking vlan</a>	Displays information about the explicit host tracking for IGMPv3 hosts.

## ip igmp snooping mrouter

To configure a Layer 2 port as a multicast router port, use the **ip igmp snooping mrouter** command. To remove the configuration, use the **no** form of this command

```
ip igmp snooping mrouter {interface {interface interface-number} |
  {port-channel number}} | {learn {cgmp | pim-dvmrp}}
```

```
no ip igmp snooping mrouter {interface {interface interface-number} |
  {port-channel number}} | {learn {cgmp | pim-dvmrp}}
```

Syntax Description		
<b>interface</b>		Specifies the next-hop interface to the multicast router.
<i>interface</i>		Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , and <b>tengigabitethernet</b> . See the “Usage Guidelines” section for additional valid values.
<i>interface-number</i>		Module and port number; see the “Usage Guidelines” section for valid values.
<b>port-channel</b> <i>number</i>		Specifies the port-channel number; valid values are a maximum of 64 values ranging from 1 to 256.
<b>learn</b>		Specifies the learning method for the multicast router.
<b>cgmp</b>		Specifies the snooping CGMP packets for the multicast router.
<b>pim-dvmrp</b>		Specifies the snooping PIM-DVMRP packets for the multicast router.

**Defaults** **pim-dvmrp**

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Enter this command in VLAN interface configuration mode only.

The interface to the router must be in the VLAN where you are entering the command, the interface must be administratively up, and the line protocol must be up.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The CGMP learning method can decrease control traffic.

The learning method that you configure is saved in NVRAM.

Static connections to multicast routers are supported only on switch ports.

**Examples**

This example shows how to specify the next-hop interface to the multicast router:

```
Router(config-if)# ip igmp snooping mrouter interface fastethernet 5/6
Router(config-if)#
```

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

```
Router(config-if)# ip igmp snooping mrouter learn cgmp
Router(config-if)#
```

**Related Commands**

Command	Description
<b>ip igmp snooping</b>	Enables IGMP snooping.
<b>ip igmp snooping fast-leave</b>	Enables the IGMPv3-snooping fast-leave processing.
<b>show ip igmp snooping mrouter</b>	Displays the information about the dynamically learned and manually configured multicast router interfaces.

# ip igmp snooping querier

To enable multicast support within a subnet when no multicast routing protocol is configured in the VLAN or subnet, use the **ip igmp snooping querier** command. To disable multicast support within a subnet when no multicast routing protocol is configured, use the **no** form of this command.

**ip igmp snooping querier**

**no ip igmp snooping querier**

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

**Defaults** Disabled

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

Enter this command in VLAN interface configuration mode only.

You enable IGMP snooping on the Catalyst 6500 series switch, and disable PIM on the VLAN. Configure the VLAN in global configuration mode.

Configure an IP address on the VLAN interface. When enabled, the IGMP-snooping querier uses the IP address as the query source address. If no IP address is configured on the VLAN interface, the IGMP-snooping querier does not start. The IGMP-snooping querier disables itself if you clear the IP address. When enabled, the IGMP-snooping querier restarts if you configure an IP address.

The IGMP-snooping querier supports IGMPv2.

When enabled, the IGMP-snooping querier does the following:

- Does not start if it detects IGMP traffic from a multicast router.
- Starts after 60 seconds when no IGMP traffic is detected from a multicast router.
- Disables itself if it detects IGMP traffic from a multicast router.

QoS does not support IGMP packets when IGMP snooping is enabled.

You can enable the IGMP-snooping querier on all the Catalyst 6500 series switches in the VLAN. One Catalyst 6500 series switch is elected as the querier.

If multicast routers are not present on the VLAN or subnet, the Catalyst 6500 series switch becomes the IGMP querier for the VLAN when you enable the IGMP-snooping querier.

If you disable the IGMP-snooping querier, IGMP snooping functions only when you configure PIM in the subnet.

You can enter the **ip igmp snooping querier** command at any time, but the IGMP-snooping querier starts only when no other multicast routers are present in the VLAN or subnet.

You can use this command as an alternative to configuring PIM in a subnet; use this command when the multicast traffic does not need to be routed but you would like support for IGMP snooping on Layer 2 interfaces in your network.

---

### Examples

This example shows how to enable the IGMP-snooping querier on the VLAN:

```
Router(config-if)# ip igmp snooping querier
Router(config-if)#
```

---

### Related Commands

Command	Description
<a href="#">show ip igmp snooping mrouter</a>	Displays the information about the dynamically learned and manually configured multicast router interfaces.

# ip igmp snooping rate

To set the rate limit for IGMP-snooping packets, use the **ip igmp snooping rate** command. To disable the software rate limiting, use the **no** form of this command.

**ip igmp snooping rate** *pps*

**no ip igmp snooping rate**

<b>Syntax Description</b>	<i>pps</i> Rate limit of incoming IGMP messages; valid values are from 100 to 6000 packets per second.				
<b>Defaults</b>	Disabled				
<b>Command Modes</b>	Global configuration				
<b>Command History</b>	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Release</th> <th style="text-align: left;">Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(18)ZY</td> <td>Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)ZY	Support for this command was introduced.
Release	Modification				
12.2(18)ZY	Support for this command was introduced.				
<b>Examples</b>	<p>This example shows how to enable software rate limiting:</p> <pre>Router(config)# ip igmp snooping rate Router(config)#</pre> <p>This example shows how to disable software rate limiting:</p> <pre>Router(config)# no ip igmp snooping rate Router(config)#</pre>				
<b>Related Commands</b>	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Command</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td><a href="#">show ip igmp snooping rate-limit</a></td> <td>Displays the information about the IGMP snooping rate limit.</td> </tr> </tbody> </table>	Command	Description	<a href="#">show ip igmp snooping rate-limit</a>	Displays the information about the IGMP snooping rate limit.
Command	Description				
<a href="#">show ip igmp snooping rate-limit</a>	Displays the information about the IGMP snooping rate limit.				

# ip igmp snooping report-suppression

To turn on IP IGMP snooping report suppression, use the **ip igmp snooping report-suppression** command. To turn off report suppression, use the **no** form of this command.

**ip igmp snooping report-suppression**

**no ip igmp snooping report-suppression**

---

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

---

**Defaults** Disabled

---

**Command Modes** Interface configuration

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Usage Guidelines** When you enable report suppression for all host reports responding to a general query, IP IGMP snooping forwards the first report only and suppresses the remaining reports to constrain IGMP traffic to the multicast router.

# ip igmp snooping source-only-learning age-timer

To flood multicast packets periodically to a Layer 2 segment that has only multicast sources and no receivers connected to it, use the **ip igmp snooping source-only-learning age-timer** command. To return to the default settings, use the **no** form of this command.

**ip igmp snooping source-only-learning age-timer** *seconds*

**no ip igmp snooping source-only-learning age-timer**

## Syntax Description

<i>seconds</i>	Source-only entries age timer value in seconds; valid values are from 0 to 86400 seconds.
----------------	---

## Defaults

*seconds* is **600** seconds (10 minutes).

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

There are two source-only timers that run in an alternating fashion; the `source_only_age_timer` and the `source_only_delete_timer`. The value that you configure by entering the **ip igmp snooping source-only-learning age-timer** command sets the `source_only_age_timer`. The `source_only_delete_timer` has a fixed, nonconfigurable value of 5 minutes (300 seconds).

The expiration of one timer starts the other timer. At any time, only one timer is running.

Setting the age timer to **0** stops the flooding in the source-only VLAN.



### Note

Setting the age timer to a nonzero value causes flooding to occur every x (configured value) + 5 minutes (`source_only_delete_timer`) interval.

## Examples

This example shows how to flood multicast packets periodically:

```
Router(config)# ip igmp snooping source-only-learning age-timer 300
Router(config)#
```

This example shows how to return to the default settings:

```
Router(config)# no ip igmp snooping source-only-learning age-timer
Router(config)#
```

## ip igmp ssm-map

To enable and configure SSM mapping, use the **ip igmp ssm-map** command. To disable SSM mapping, use the **no** form of this command.

```
ip igmp ssm-map {enable | {query dns} | {static {group-access-list | group-access-list-name}
source-address}}
```

```
no ip igmp ssm-map {enable | {query dns}}
```

### Syntax Description

<b>enable</b>	Enables SSM group to the source mapping.
<b>query dns</b>	Enables the DNS lookup.
<b>static</b>	Specifies an SSM static group to the source mapping.
<i>group-access-list</i>	Group access list to map to the source address.
<i>group-access-list-name</i>	Name of the group access list to map to the source address.
<i>source-address</i>	Source address.

### Defaults

Disabled

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

By default, the locally configured static SSM mappings and the DNS server are queried. Local configured mappings have priority over dynamic mappings. If a DNS server is not available, you may want to disable DNS server lookups. To disable DNS lookups, use the **no ip igmp ssm-map query dns** command.

If a DNS server is not available, a locally configured static SSM mapping database is used to query. A database query uses the group address and receives the source list in return. As soon as the static SSM mappings are configured, the maps are used for the lookups. To build a static SSM mappings database, use the following commands:

```
ip igmp ssm-map static acl-1 source-1-ip-address
```

```
ip igmp ssm-map static acl-2 source-2-ip-address
```

The ACL specifies the group or groups that have to be mapped to the listed source. Because the content servers may send out more than one stream with the same source address, the access list is used to group the multicast destination addresses together. You can use wildcards if the addresses are contiguous.

If multiple sources have to be joined for a multicast group address, you must place the group in all ACLs that are associated with the source address. In the example above, if group G must join sources 1 and 2, the group address must be placed in both acl-1 and acl-2.

When you enable SSM mapping using the **ip igmp ssm-map enable** command, but the source mapping list is empty for the group, enter the **no ip igmp ssm-map query dns** command. The **ip igmp ssm-map enable** command is supported on statically configured SSM-mapped source entries only.

---

## Examples

This example shows how to enable an SSM group to the source mapping:

```
Router(config)# ip igmp ssm-map enable
Router(config)#
```

This example shows how to enable DNS lookups:

```
Router(config)# ip igmp ssm-map query dns
Router(config)#
```

This example shows how to build a static SSM mapping database:

```
Router(config)# ip igmp ssm-map static acl1 255.255.255.0
Router(config)# ip igmp ssm-map static acl2 255.255.255.0
Router(config)#
```

This example shows how to disable an SSM group to the source mapping:

```
Router(config)# no ip igmp ssm-map enable
Router(config)#
```

This example shows how to disable DNS lookups:

```
Router(config)# no ip igmp ssm-map query dns
Router(config)#
```

# ip local-proxy-arp

To enable local-proxy ARP, use the **ip local-proxy-arp** command. To disable local-proxy ARP, 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** Disabled

---

**Command Modes** Interface configuration

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Usage Guidelines** Use local-proxy ARP on subnets where the hosts are intentionally prevented from communicating directly with each other; for example, you can use local-proxy ARP in private VLAN environments. Local-proxy ARP allows the PISA to respond to ARP requests for IP addresses within a subnet where normally no routing is required. When you enable local-proxy ARP, the PISA can respond to ARP requests for IP addresses within a common subnet where traffic is not normally routed. This situation happens only when two hosts on the same subnet cannot directly ARP for each other.

ICMP redirects are disabled on interfaces where local-proxy ARP is enabled.

---

**Examples** This example shows how to enable local-proxy ARP:

```
Router(config-if)# ip local-proxy-arp
Router(config-if)#s
```

# ip mroute

To configure a multicast static route (mroute), use the **ip mroute** command. To remove the route, use the **no** form of this command.

**ip mroute** [**vrf** *vrf-name*] *source-address mask* [*protocol as-number*] {*rpf-address* | *interface-type interface-number*} [*distance*]

**no ip mroute** [**vrf** *vrf-name*] *source-address mask* [*protocol as-number*] {*rpf-address* | *interface-type interface-number*} [*distance*]

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
<i>source-address</i>	IP address of the multicast source.	
<i>mask</i>	Mask on the IP address of the multicast source.	
<i>protocol</i>	(Optional) Unicast routing protocol that you are using.	
<i>as-number</i>	(Optional) Autonomous system number of the routing protocol that you are using, if applicable.	
<i>rpf-address</i>	Incoming interface for the mroute.	
<i>interface-type</i> <i>interface-number</i>	Interface type and number for the mroute.	
<i>distance</i>	(Optional) Administrative distance; valid values are from 0 to 255.	

**Defaults** *distance* is 0.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command allows you to statically configure where multicast sources are located (even though the unicast routing table shows something different).

When a source range is specified, the *rpf-address* argument applies only to those sources.

If the *rpf-address* is a PIM neighbor, PIM join, graft, and prune messages are sent to it. The *rpf-address* argument can be a host IP address of a directly connected system or a network/subnet number. When it is a route, a recursive lookup is done from the unicast routing table to find a directly connected system. If the *rpf-address* argument is not specified, the interface *interface-type interface-number* value is used as the incoming interface.

The *distance* argument determines whether a unicast route, a DVMRP route, or a static mroute is used for the RPF lookup. The lower distances have a higher priority. If the static mroute has the same distance as the other two RPF sources, the static mroute will take precedence.

---

**Examples**

This example shows how to configure all sources from a single interface (in this case, a tunnel):

```
Router(config)# ip mroute 224.0.0.0 255.255.255.255 tunnel0
Router(config)#
```

This example shows how to configure all specific sources within a network number to be reachable through 172.30.10.13:

```
Router(config)# ip mroute 172.16.0.0 255.255.0.0 172.30.10.13
Router(config)#
```

This example shows how to cause this multicast static route to take effect if the unicast routes for any given destination is deleted:

```
Router(config)# ip mroute 224.0.0.0 255.255.255.255 serial0 200
Router(config)#
```

## ip msdp border

To configure a router that borders a PIM sparse-mode region and dense-mode region to use MSDP, use the **ip msdp border** command. To prevent this action, use the **no** form of this command.

```
ip msdp [vrf vrf-name] border sa-address internet-type internet-number
```

```
no ip msdp [vrf vrf-name] border sa-address internet-type internet-number
```

### Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
<b>sa-address</b>	Specifies an active source IP address.
<i>internet-type internet-number</i>	Interface type and number from which the IP address is derived and used as the rendezvous-point address in source-active messages.

### Defaults

The active sources in the dense-mode region will not participate in MSDP.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

Use this command if you want the router to send source-active messages for sources active in the PIM dense-mode region to MSDP peers.

Specifying the *internet-type internet-number* allows the MSDP peers to forward source-active messages away from this border. The IP address of the interface is used as the originator ID, which is the rendezvous point field in the MSDP source-active message.



#### Note

We recommend that you configure the border router in the sparse-mode domain to proxy-register sources in the dense-mode domain and configure the sparse-mode domain to use standard MSDP procedures to advertise these sources.



#### Note

If you use this command, you must limit the sources advertised by using the **ip msdp redistribute** command. Configure the **ip msdp redistribute** command to apply to only local sources. Be aware that this configuration can result in an (S,G) state that remains long after a source in the dense-mode domain has stopped sending.

**Note**

The **ip msdp originator-id** command identifies an interface type and number to be used as the rendezvous-point address. If both the **ip msdp border** and **ip msdp originator-id** commands are configured, the **ip msdp originator-id** command prevails. The address derived from the **ip msdp originator-id** command determines the address of the rendezvous point.

**Examples**

In this example, the local router is not a rendezvous point; it borders a PIM sparse-mode region with a dense-mode region and uses the IP address of Ethernet interface 0 as the rendezvous point address in source-active messages.

```
Router(config)# ip msdp border sa-address ethernet0
Router(config)#
```

**Related Commands**

Command	Description
<b>ip msdp originator-id</b>	Allows an MSDP speaker that originates a source-active message to use the IP address of the interface as the rendezvous-point address in the source-active message.
<b>ip msdp redistribute</b>	Configures which (S,G) entries from the multicast routing table are advertised in source-active messages originated to MSDP peers.

# ip msdp cache-sa-state

To create a source-active state on the router, use the **ip msdp cache-sa-state** command.

**ip msdp cache-sa-state** [**vrf** *vrf-name*]

<b>Syntax Description</b>	<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
---------------------------	----------------------------	--

<b>Defaults</b>	The router creates the source-active state for all MSDP source-active messages that it receives.
-----------------	--

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	This command is automatically configured if at least one MSDP peer is configured. It cannot be disabled.
-------------------------	--

<b>Examples</b>	This example shows how the <b>ip msdp cache-sa-state</b> command is enabled when an MSDP peer is configured. For more MSDP configuration examples, refer to the “Configuring Multicast Source Discovery Protocol” chapter in the Cisco IOS Release 12.2 <i>Cisco IOS IP Configuration Guide</i> .
-----------------	---

```

1
1
1
Router(config)# ip classless
Router(config)# ip msdp peer 192.168.1.2 connect-source Loopback0
Router(config)# ip msdp peer 192.169.1.7
Router(config)# ip msdp mesh-group outside-test 192.168.1.2
Router(config)# ip msdp cache-sa-state
Router(config)# ip msdp originator-id Loopback0
1
1
1

```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">clear ip msdp sa-cache</a>	Configures an MSDP peer.
	<a href="#">ip msdp filter-sa-request</a>	Creates a source-active state on the router.
	<a href="#">show ip msdp sa-cache</a>	Displays (S, G) state learned from MSDP peers.

## ip msdp default-peer

To define a default peer from which to accept all MSDP source-active messages, use the **ip msdp default-peer** command. To remove the default peer, use the **no** form of this command.

```
ip msdp [vrf vrf-name] default-peer {peer-address | peer-name} [prefix-list list]
```

```
no ip msdp [vrf vrf-name] default-peer
```

Syntax Description	<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
	<i>peer-address</i>   <i>peer-name</i>	IP address or DNS name of the MSDP default peer.
	<b>prefix-list</b> <i>list</i>	(Optional) Specifies the BGP prefix list.

**Defaults** No default MSDP peer exists.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Use the **ip msdp default-peer** command if you do not want to configure your MSDP peer to be a BGP peer also.

If only one MSDP peer is configured (with the **ip msdp peer** command), it will be used as a default peer. You do not need to configure a default peer with this command.

If you do not specify the **prefix-list list** keyword and argument, all source-active messages that are received from the configured default peer are accepted.

The **prefix-list list** keyword and argument specifies that the peer will be a default peer only for the prefixes listed in the list specified by the *list* argument. You must configure a BGP prefix list for this **prefix-list list** keyword and argument to have any effect.

You should configure a BGP prefix list if you intend to configure the **prefix-list list** keyword and argument with the **ip msdp default-peer** command.

If you specify the **prefix-list list** keyword and argument, the source-active messages that originated from the rendezvous points that are covered by the **prefix-list list** keyword and argument are accepted from the configured default peer. If you specify the **prefix-list list** keyword and argument but do not configure a prefix list, the default peer is used for all prefixes.

You can enter multiple **ip msdp default-peer** commands, with or without the **prefix-list** keyword. However, all commands must either have the keyword or all must not have the keyword.

- When you use multiple **ip msdp default-peer** commands with the **prefix-list** keyword, you use all the default peers at the same time for different rendezvous-point prefixes. This syntax is typically used in a service provider cloud that connects stub site clouds.
- When you use multiple **ip msdp default-peer** commands without the **prefix-list** keyword, you use a single active peer to accept all source-active messages. If that peer goes down, then you move to the next configured default peer to accept all source-active messages. This syntax is typically used at a stub site.

## Examples

This example shows how to configure the router named router.cisco.com as the default peer to the local router:

```
Router(config)# ip msdp peer 192.168.1.2
Router(config)# ip msdp peer 192.168.1.3
Router(config)# ip msdp default-peer router.cisco.com !At a stub site
```

This example shows how to configure the router at IP address 192.168.1.3 as the default peer to the local router:

```
Router(config)# ip msdp peer 192.168.1.3
Router(config)# ip msdp peer 192.168.3.5
Router(config)# ip msdp default-peer 192.168.1.3
```

This example shows how to configure two default peers:

```
Router(config)# ip msdp peer 172.18.2.3
Router(config)# ip msdp peer 172.19.3.5
Router(config)# ip msdp default-peer 172.18.2.3 prefix-list site-c
Router(config)# ip prefix-list site-a permit 172.18.0.0/16
Router(config)# ip msdp default-peer 172.19.3.5 prefix-list site-a
Router(config)# ip prefix-list site-c permit 172.19.0.0/16
```

## Related Commands

Command	Description
<a href="#">ip msdp peer</a>	Configures an MSDP peer.
<a href="#">ip prefix-list</a>	Creates an entry in a prefix list.

# ip msdp description

To add descriptive text to the configuration for an MSDP peer, use the **ip msdp description** command. To remove the description, use the **no** form of this command.

```
ip msdp [vrf vrf-name] description {peer-name | peer-address} text
```

```
no ip msdp [vrf vrf-name] description {peer-name | peer-address}
```

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
<i>peer-name</i>   <i>peer-address</i>	Peer name or address to which this description applies.	
<i>text</i>	Description of the MSDP peer.	

**Defaults** No description is associated with an MSDP peer.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Configure a description to make the MSDP peer easier to identify. This description is displayed in the output of the **show ip msdp peer** command.

**Examples** This example shows how to configure the router at the IP address 224.107.5.4 with a description indicating it is a router at customer A:

```
Router(config)# ip msdp description 224.107.5.4 router at customer a
Router(config)#
```

Related Commands	Command	Description
	<b>show ip msdp peer</b>	Displays detailed information about the MSDP peer.

# ip msdp filter-sa-request

To configure the router to send source-active request messages to the MSDP peer when a new joiner from a group becomes active, use the **ip msdp filter-sa-request** command. To prevent this action, use the **no** form of this command.

```
ip msdp [vrf vrf-name] filter-sa-request {peer-address | peer-name} [list access-list]
```

```
no ip msdp [vrf vrf-name] filter-sa-request {peer-address | peer-name}
```

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
<i>peer-address</i>	IP address of the MSDP peer from which the local router requests source-active messages when a new joiner for the group becomes active.	
<i>peer-name</i>	Name of the MSDP peer from which the local router requests source-active messages when a new joiner for the group becomes active.	
<b>list</b> <i>access-list</i>	(Optional) Specifies the standard IP access-list number or name that describes a multicast group address.	

**Defaults** If this command is not configured, all source-active request messages are recognized. If this command is configured but no access list is specified, all source-active request messages are ignored.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** By default, the router recognizes all source-active request messages from peers. Use this command if you want to control exactly which source-active request messages that the router will recognize.

If no access list is specified, all source-active request messages are ignored. If an access list is specified, only source-active request messages from those permitted groups will be recognized, and all others will be ignored.

**Examples** This example shows how to configure the router to filter source-active request messages from the MSDP peer at 172.16.2.2. This example also shows that the source-active request messages from sources on the network 192.168.22.0 pass access list 1 and will be recognized; all others will be ignored.

```
Router(config)# ip msdp filter sa-request 224.69.2.2 list 1
access-list 1 permit 228.4.22.0 0.0.0.255
```

## ■ ip msdp filter-sa-request

Related Commands	Command	Description
	<a href="#">ip msdp peer</a>	Configures an MSDP peer.

## ip msdp mesh-group

To configure an MSDP peer to be a member of a mesh group, use the **ip msdp mesh-group** command. To remove an MSDP peer from a mesh group, use the **no** form of this command.

```
ip msdp [vrf vrf-name] mesh-group mesh-name {peer-address | peer-name}
```

```
no ip msdp [vrf vrf-name] mesh-group mesh-name {peer-address | peer-name}
```

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
<i>mesh-name</i>	Name of the mesh group.	
<i>peer-address</i>   <i>peer-name</i>	IP address or name of the MSDP peer to be a member of the mesh group.	

**Defaults** The MSDP peers do not belong to a mesh group.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** A mesh group is a group of MSDP speakers that have fully meshed MSDP connectivity among themselves. The source-active messages received from a peer in a mesh group are not forwarded to the other peers in the same mesh group.

The mesh groups can be used to achieve two goals:

- Reduce source-active message flooding
- Simplify peer-RPF flooding (you do not need to run BGP or multiprotocol BGP among MSDP peers)

**Examples** This example shows how to configure the MSDP peer at address 224.1.1.1 to be a member of the mesh group named internal:

```
Router(config)# ip msdp mesh-group internal 224.1.1.1
Router(config)#
```

## ip msdp originator-id

To allow an MSDP speaker that originates a source-active message to use the IP address of the interface as the rendezvous-point address in the source-active message, use the **ip msdp originator-id** command. To prevent the rendezvous-point address from being derived in this way, use the **no** form of this command.

**ip msdp** [**vrf** *vrf-name*] **originator-id** *interface-type interface-number*

**no ip msdp** [**vrf** *vrf-name*] **originator-id** *interface-type interface-number*

### Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
<i>interface-type</i> <i>interface-number</i>	Interface type and number on the local router whose IP address is used as the rendezvous-point address in source-active messages.

### Defaults

The rendezvous-point address is used as the originator ID.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

The **ip msdp originator-id** command identifies an interface type and number to be used as the rendezvous-point address in a source-active message.

Use this command if you want to configure a logical rendezvous point. Because only rendezvous points and MSDP border routers originate source-active messages, you might need to change the ID used for this purpose.

If both the **ip msdp border sa-address** and **ip msdp originator-id** commands are configured, the **ip msdp originator-id** command prevails. The address derived from the **ip msdp originator-id** command determines the address of the rendezvous point to be used in the source-active message.

### Examples

This example shows how to configure the IP address of Ethernet interface 1 as the rendezvous-point address in source-active messages:

```
Router(config)# ip msdp originator-id ethernet1
Router(config)#
```

### Related Commands

Command	Description
<a href="#">ip msdp border</a>	Configures a router that borders a PIM sparse-mode region and dense-mode region to use MSDP.

# ip msdp peer

To configure an MSDP peer, use the **ip msdp peer** command. To remove the peer relationship, use the **no** form of this command.

```
ip msdp [vrf vrf-name] peer {peer-name | peer-address} [connect-source interface-type
interface-number] [remote-as as-number]
```

```
no ip msdp [vrf vrf-name] peer {peer-name | peer-address}
```

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
<i>peer-name</i>   <i>peer-address</i>	DNS name or IP address of the router that is to be the MSDP peer.	
<b>connect-source</b> <i>interface-type</i> <i>interface-number</i>	(Optional) Specifies the interface type and number whose primary address becomes the source IP address for the TCP connection.	
<b>remote-as</b> <i>as-number</i>	(Optional) Specifies the autonomous system number of the MSDP peer.	

**Defaults** No MSDP peer is configured.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The router specified should also be configured as a BGP neighbor. The *interface-type* is on the router being configured.

If you are also using BGP peering with this MSDP peer, you should use the same IP address for MSDP that you used for BGP. However, you are not required to run BGP or multiprotocol BGP with the MSDP peer if there is a BGP or MBGP path between the MSDP peers. If there is no path, you must configure the **ip msdp default-peer** command.

The **remote-as** *as-number* keyword and argument is used for display purposes only.

A peer might appear to be in another autonomous system (other than the one it really resides in) when you have an MSDP peering session but do not have a BGP peer session with that peer. In this case, if the prefix of the peer is injected by another autonomous system, it displays as the autonomous system number of the peer.

**Examples**

This example shows how to configure the router at the IP address 224.108.1.2 as an MSDP peer to the local router. The neighbor belongs to autonomous system 109.

```
Router(config)# ip msdp peer 224.108.1.2 connect-source ethernet 0
router bgp 110
 network 224.108.0.0
 neighbor 224.108.1.2 remote-as 109
 neighbor 224.108.1.2 update-source ethernet 0
```

This example shows how to configure the router named router.cisco.com as an MSDP peer to the local router:

```
Router(config)# ip msdp peer router.cisco.com
Router(config)#
```

This example shows how to configure the router named router.cisco.com to be an MSDP peer in autonomous system 109. The primary address of Ethernet interface 0 is used as the source address for the TCP connection.

```
Router(config)# ip msdp peer router.cisco.com connect-source ethernet0 remote-as 109
Router(config)#
```

**Related Commands**

Command	Description
<b>neighbor remote-as</b>	Adds an entry to the BGP or multiprotocol BGP neighbor table.

# ip msdp redistribute

To configure which (S,G) entries from the multicast routing table are advertised in source-active messages originated to MSDP peers, use the **ip msdp redistribute** command. To remove the filter, use the **no** form of this command.

```
ip msdp [vrf vrf-name] redistribute [list access-list-name] [asn as-access-list-number]
[route-map map-name]
```

```
no ip msdp [vrf vrf-name] redistribute
```

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
<b>list</b> <i>access-list-name</i>	(Optional) Specifies the standard or extended IP access-list number or name that controls which local sources are advertised and to which groups they send.	
<b>asn</b> <i>as-access-list-number</i>	(Optional) Specifies the standard or extended IP access-list number; valid values are from 1 to 199.	
<b>route-map</b> <i>map-name</i>	(Optional) Specifies the route-map name.	

## Defaults

The default settings are as follows:

- If no portion of this command is configured, only local sources are advertised, provided that they send to groups for which the router is a rendezvous point.
- If no portion of this command is configured and if the **ip msdp border sa-address** command is configured, all local sources are advertised.
- If the **ip msdp redistribute** command is configured with no keywords, no multicast sources are advertised.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

You must configure the *as-access-list-number* argument in the **ip as-path** command.

This command affects source-active message origination, not source-active message forwarding. If you want to filter which source-active messages are forwarded to MSDP peers, use the **ip msdp sa-filter in** or **ip msdp sa-filter out** command.

The **ip msdp redistribute** command controls which (S,G) pairs the router advertises from the multicast routing table. By default, only sources within the local domain are advertised. Use the following guidelines for the **ip msdp redistribute** command:

- If you specify the **list** *access-list-name* keyword and argument only, you filter which local sources are advertised and to which groups are sent advertisements. The access list specifies a source address, source mask, group address, and group mask.
- If you specify the **asn** *as-access-list-number* keyword and argument only, you advertise all sources sending to any group that pass through the autonomous system path access list. The autonomous system path access-list number refers to the **ip as-path** command, which specifies an access list. If you specify the **asn 0** keywords, sources from all autonomous systems are advertised. The **asn 0** keywords are useful when connecting dense-mode domains to a sparse-mode domain running MSDP, or when using MSDP in a router that is not configured with BGP. In these cases, you do not know if a source is local.
- If you specify the **route-map** *map-name* keyword and argument only, you advertise all sources that satisfy the match criteria in the route map *map-name* argument.
- If you specify all three keywords (**list**, **asn**, and **route-map**), all conditions must be true before any multicast source is advertised in a source-active message.
- If you specify the **ip multicast redistribute** command with no other keywords or arguments, no multicast sources are advertised.

### Examples

This example shows how to configure which (S,G) entries from the multicast routing table are advertised in source-active messages originated to MSDP peers:

```
Router(config)# ip msdp redistribute route-map customer-sources

route-map customer-sources permit
match as-path customer-as

Router(config)# ip as-path access-list ^109$
```

### Related Commands

Command	Description
<b>ip as-path</b>	Defines a BGP autonomous system path access list.
<b>ip msdp border</b>	Configures a router that borders a PIM sparse-mode region and dense-mode region to use MSDP.

## ip msdp sa-filter in

To configure an incoming filter list for source-active messages received from the specified MSDP peer, use the **ip msdp sa-filter in** command. To remove the filter, use the **no** form of this command.

```
ip msdp [vrf vrf-name] sa-filter in {peer-address | peer-name} [list access-list-name] [route-map map-name]
```

```
no ip msdp [vrf vrf-name] sa-filter in {peer-address | peer-name} [list access-list-name] [route-map map-name]
```

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
<i>peer-address</i>   <i>peer-name</i>	IP address or name of the MSDP peer from which the source-active messages are filtered.	
<b>list</b> <i>access-list-name</i>	(Optional) Specifies the IP access-list number or name.	
<b>route-map</b> <i>map-name</i>	(Optional) Specifies the route-map name.	

### Defaults

The default settings are as follows:

- If this command is not configured, no incoming messages are filtered; all source-active messages are accepted from the peer.
- If the command is configured, but no access list or route map is specified, all source/group pairs from the peer are filtered.
- If both the **list** and **route-map** keywords are used, all conditions must be true to pass any (S,G) pair in incoming source-active messages.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

If you do not specify an *access-list-name*, all source/group pairs from the peer are filtered.

The specified MSDP peer passes only those source-active messages that meet the match criteria in the route map *map-name* argument.

If all match criteria are true, a **permit** keyword from the route map passes the routes through the filter. Use the **deny** keyword to filter the routes.

## ■ ip msdp sa-filter in

**Examples**

This example shows how to configure the router to filter all source-active messages from the peer named router.cisco.com:

```
Router(config)# ip msdp peer router.cisco.com connect-source ethernet 0
Router(config)# ip msdp sa-filter in router.cisco.com
Router(config)#
```

**Related Commands**

Command	Description
<a href="#">ip msdp peer</a>	Configures an MSDP peer.
<a href="#">ip msdp sa-filter out</a>	Configures an outgoing filter list for source-active messages sent to the specified MSDP peer.

## ip msdp sa-filter out

To configure an outgoing filter list for source-active messages sent to the specified MSDP peer, use the **ip msdp sa-filter out** command. To remove the filter, use the **no** form of this command.

```
ip msdp [vrf vrf-name] sa-filter out {peer-address | peer-name} [list access-list-name]
[route-map map-name]
```

```
no ip msdp [vrf vrf-name] sa-filter out {peer-address | peer-name} [list access-list-name]
[route-map map-name]
```

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
<i>peer-address</i>   <i>peer-name</i>	IP address or DNS name of the MSDP peer to which the source-active messages are filtered.	
<b>list</b> <i>access-list</i>	(Optional) Specifies the extended IP access-list number or name.	
<b>route-map</b> <i>map-name</i>	(Optional) Specifies the route map name.	

### Defaults

The default settings are as follows:

- If this command is not configured, no outgoing messages are filtered; all source-active messages received are forwarded to the peer.
- If the command is configured, but no access list or route map is specified, all source/group pairs are filtered.
- If both the **list** and **route-map** keywords are used, all conditions must be true to pass any (S,G) pairs in outgoing source-active messages.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

If you do not specify an *access-list*, all source/group pairs are filtered. The specified MSDP peer passes only those source-active messages that pass the extended access list.

If both the **list** and **route-map** keywords are used, all conditions must be true to pass any (S,G) pairs in outgoing source-active messages.

To the specified MSDP peer, only those source-active messages that meet the match criteria in the route map *map-name* argument are passed.

If all match criteria are true, a **permit** keyword from the route map passes routes through the filter. Use the **deny** keyword to filter the routes.

**Examples**

This example shows how to allow only (S,G) pairs that pass access list 100 to be forwarded in a source-active message to the peer named router.cisco.com:

```
Router(config)# ip msdp peer router.cisco.com connect-source ethernet 0
Router(config)# ip msdp sa-filter out router.cisco.com list 100
access-list 100 permit ip 224.69.0.0 0.0.255.255 224.2.0.0 0.0.255.255
```

**Related Commands**

Command	Description
<a href="#">ip msdp peer</a>	Configures an MSDP peer.
<a href="#">ip msdp sa-filter in</a>	Configures an incoming filter list for source-active messages received from the specified MSDP peer.

## ip msdp sa-request

To configure the router to send source active request messages to the MSDP peer when a new joiner from the group becomes active, use the **ip msdp sa-request** command. To prevent this action, use the **no** form of this command.

```
ip msdp [vrf vrf-name] sa-request {peer-address | peer-name}
```

```
no ip msdp [vrf vrf-name] sa-request {peer-address | peer-name}
```

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
<i>peer-address</i>   <i>peer-name</i>	IP address or name of the MSDP peer from which the local router requests source-active messages when a new joiner for the group becomes active.	

**Defaults** The router does not send source-active request messages to the MSDP peer.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** By default, the router does not send any source-active request messages to its MSDP peers when a new member joins a group and wants to receive multicast traffic. The new member waits to receive any source-active messages that eventually arrive.

Use this command if you want a new member of a group to learn the current, active multicast sources in a connected PIM-SM domain that are sending to a group. The router sends source-active request messages to the specified MSDP peer when a new member joins a group. The peer replies with the information in its source-active cache. If the peer does not have a cache configured, this command does not work.

You can also use the **ip msdp cache-sa-state** command to have the router cache messages.

**Examples** This example shows how to configure the router to send source-active request messages to the MSDP peer at 224.69.1.1:

```
Router(config)# ip msdp sa-request 224.69.1.1
Router(config)#
```

## ■ ip msdp sa-request

Related Commands	Command	Description
	<a href="#">ip msdp cache-sa-state</a>	Creates a source-active state on the router.
	<a href="#">ip msdp peer</a>	Configures an MSDP peer.

# ip msdp shutdown

To administratively shut down a configured MSDP peer, use the **ip msdp shutdown** command. To bring the peer back up, use the **no** form of this command.

```
ip msdp [vrf vrf-name] shutdown {peer-address | peer-name}
```

```
no ip msdp [vrf vrf-name] shutdown {peer-address | peer-name}
```

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
<i>peer-address</i>   <i>peer-name</i>	IP address or name of the MSDP peer to shut down.	

**Defaults** No action is taken to shut down an MSDP peer.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to shut down the MSDP peer at the IP address 224.5.7.20:

```
Router(config)# ip msdp shutdown 224.5.7.20
Router(config)#
```

Related Commands	Command	Description
	<a href="#">ip msdp peer</a>	Configures an MSDP peer.

## ip msdp ttl-threshold

To limit which multicast data packets are sent in source-active messages to an MSDP peer, use the **ip msdp ttl-threshold** command. To restore the default value, use the **no** form of this command.

```
ip msdp [vrf vrf-name] ttl-threshold {peer-address | peer-name} ttl-value
```

```
no ip msdp [vrf vrf-name] ttl-threshold {peer-address | peer-name}
```

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
<i>peer-address</i>   <i>peer-name</i>	IP address or name of the MSDP peer to which the <i>ttl-value</i> argument applies.	
<i>ttl-value</i>	Time-to-live (TTL) value; valid values are from 0 to 255.	

**Defaults** *ttl-value* is **0**.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command limits which multicast data packets are sent in data-encapsulated source-active messages. Only multicast packets with an IP header TTL greater than or equal to the *ttl-value* argument are sent to the MSDP peer that is specified by the IP address or name.

Use this command if you want to use TTL to limit your multicast data traffic. For example, you could limit internal traffic to a TTL of 8. If you want other groups to go to external locations, you need to send those packets with a TTL greater than 8.

The default value of the *ttl-value* argument is 0, which means that all multicast data packets are forwarded to the peer until the TTL is exhausted.

**Examples** This example shows how to configure a TTL threshold of eight hops:

```
Router(config)# ip msdp ttl-threshold 224.5.7.20 8
Router(config)#
```

Related Commands	Command	Description
	<a href="#">ip msdp peer</a>	Configures an MSDP peer.

# ip multicast boundary

To configure an administratively scoped boundary, use the **ip multicast boundary** command. To remove the boundary, use the **no** form of this command.

**ip multicast boundary** *access-list* [**filter-autorp**]

**no ip multicast boundary** *access-list* [**filter-autorp**]

Syntax Description		
	<i>access-list</i>	Number or name that identifies an access list that controls the range of group addresses affected by the boundary.
	<b>filter-autorp</b>	(Optional) Filters auto RP messages denied by the boundary ACL.

**Defaults** There is no boundary.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Use this command to configure an administratively scoped boundary on an interface to filter the multicast group addresses in the range that is defined by the *access-list* argument. A standard access list defines the range of addresses affected. When you configure this command, multicast data packets are not allowed to flow across an interface from either direction. Restricting the multicast data packet flow enables reuse of the same multicast group address in different administrative domains.



**Note** Extended access lists are not allowed with the **filter-autorp** keyword or the use of **no** keywords.

If you configure the **filter-autorp** keyword, the administratively scoped boundary also examines Auto-RP discovery and announcement messages and removes any Auto-RP group range announcements from the Auto-RP packets that are denied by the boundary ACL. An Auto-RP group range announcement is permitted and passed by the boundary only if all addresses in the Auto-RP group range are permitted by the boundary ACL. If any address is not permitted, the entire group range is filtered and removed from the Auto-RP message before the Auto-RP message is forwarded.

Use the following guidelines when you enter the **ip multicast boundary** command:

- Only standard access lists are permitted with the use of the **filter-autorp** keyword or **no** keyword.
- All instances of the command apply to both control and data plane traffic.
- Protocol information on the extended access list is parsed to allow reuse and filtering for IOS consistency. An (S,G) operation will be filtered by an extended access list under all conditions stated above for keywords if the access list filters (S,G) traffic for all protocols.

**Examples**

This example shows how to set up a boundary for all administratively scoped addresses:

```
Router(config-if)# ip multicast boundary 1
Router(config-if)#
```

This example shows how to set up a boundary for an extended ACL:

```
Router(config-if)# ip multicast boundary 101
Router(config-if)#
```

This example shows how to filter auto RP messages denied by the boundary ACL.

```
Router(config-if)# ip multicast boundary acc_grp10 filter-autorp
Router(config-if)#
```

**Related Commands**

Command	Description
<b>access-list (IP standard)</b>	Defines a standard IP access list.

# ip multicast cache-headers

To allocate a circular buffer to store IP multicast packet headers that the router receives, use the **ip multicast cache-headers** command. To remove the buffer, use the **no** form of this command.

**ip multicast** [*vrf vrf-name*] **cache-headers** [*rtp*]

**no ip multicast** [*vrf vrf-name*] **cache-headers**

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
<b>rtp</b>	(Optional) Caches RTP headers.	

**Defaults** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** You can store IP multicast packet headers in a cache and then display them to determine the following information:

- Who is sending IP multicast packets to which groups
- Interpacket delay
- Duplicate IP multicast packets (if any)
- Multicast forwarding loops in your network (if any)
- Size of the group
- UDP port numbers
- Packet length



**Note**

This command allocates a circular buffer of approximately 32 KB. Do not configure this command if you are low on memory.

Use the **show ip mpacket** command to display the buffer.

---

**Examples**

This example shows how to allocate a buffer to store IP multicast packet headers:

```
Router(config)# ip multicast cache-headers
Router(config)#
```

---

**Related Commands**

Command	Description
<b>show ip mpacket</b>	Displays the contents of the circular cache-header buffer.

---

# ip multicast helper-map

To allow IP multicast routing in a multicast-capable internetwork between two broadcast-only internetworks, use the **ip multicast helper-map** command. To disable this function, use the **no** form of this command.

**ip multicast helper-map broadcast** *multicast-address access-list* [**ttl** *x*]

**no ip multicast helper-map broadcast** *multicast-address access-list*

## Syntax Description

<b>broadcast</b>	Specifies that the traffic is being converted from broadcast to multicast. Use this keyword with the <i>multicast-address</i> argument.
<i>multicast-address</i>	IP multicast address to which the converted traffic is directed. Use this argument with the <b>broadcast</b> keyword.
<i>access-list</i>	IP-extended access-list number or name that controls which broadcast packets are translated, based on the UDP port number.
<b>ttl</b> <i>x</i>	(Optional) Translates packets with a TTL of 1 and resets the TTL; valid values are from 1 to 50.

## Defaults

No conversion between broadcast and multicast occurs.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

When a multicast-capable internetwork is between two broadcast-only internetworks, you can convert the broadcast traffic to multicast at the first-hop router, and convert it back to broadcast at the last-hop router before delivering the packets to the broadcast clients. However, broadcast packets with the IP source address of 0.0.0.0 (such as a DHCP request) are not translated to any multicast group.

If you send a directed broadcast to the subnet, the outgoing interface of the last-hop router can be configured with an IP broadcast address of x.x.x.255, where x.x.x.0 is the subnet that you are trying to reach; otherwise, the packet is converted to 255.255.255.255.

Broadcast packets with a TTL of 1 are not translated by the **ip multicast helper-map** command unless you use the **ttl** keyword with the command.

**Examples**

This example shows how to allow IP multicast routing in a multicast-capable internetwork between two broadcast-only internetworks:

```
Router(config-if)# ip multicast helper-map broadcast 224.5.5.5 120 ttl 2
Router(config-if)#
```

**Related Commands**

Command	Description
<b>ip directed-broadcast</b>	Enables the translation of a directed broadcast to physical broadcasts.
<b>ip forward-protocol turbo-flood</b>	Speeds up the flooding of UDP packets using the spanning-tree algorithm.

# ip multicast mrinfo-filter

To filter multicast router information (mrinfo) request packets, use the **ip multicast mrinfo-filter** command. To disable this configuration, use the **no** form of this command.

**ip multicast mrinfo-filter** *access-list*

**no ip multicast mrinfo-filter** *access-list*

<b>Syntax Description</b>	<i>access-list</i> Access list of the source IP address to be filtered.				
<b>Defaults</b>	This command has no default settings.				
<b>Command Modes</b>	Global configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Release</th> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border-bottom: 1px solid black;">12.2(18)ZY</td> <td style="border-bottom: 1px solid black;">Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)ZY	Support for this command was introduced.
Release	Modification				
12.2(18)ZY	Support for this command was introduced.				
<b>Usage Guidelines</b>	The <b>ip multicast mrinfo-filter</b> command filters the mrinfo request packets for all of the sources listed in the specified access list.				
<b>Examples</b>	<p>This example shows how to specify that mrinfo request packets are filtered for all sources that are listed in access-list number 4:</p> <pre>Router(config)# ip multicast mrinfo-filter 4 Router(config)#</pre>				

# ip multicast multipath

To split the load of IP multicast traffic across multiple equal-cost paths, use the **ip multicast multipath** command. To disable this configuration, use the **no** form of this command.

**ip multicast [vrf vrf-name] multipath**

**no ip multicast [vrf vrf-name] multipath**

## Syntax Description

<b>vrf vrf-name</b>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
---------------------	--

## Defaults

If multiple equal-cost paths exist, multicast traffic will not be split across these paths.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

If you enter the **ip multicast multipath** command and multiple equal-cost paths exist in your network, load splitting will occur across the equal-cost paths for multicast traffic from different sources to the same multicast group, but not for traffic from the same source to different multicast groups. Because this command changes the way a RPF neighbor is selected, you must split the load of IP multicast traffic across equal-cost paths consistently on all routers in a redundant topology to avoid looping.

## Examples

This example shows how to split the load of IP multicast traffic across multiple equal-cost paths:

```
Router(config)# ip multicast multipath
Router(config)#
```

## Related Commands

Command	Description
<b>show ip rpf</b>	Displays the triggered RPF statistics.

# ip multicast netflow

To enable multicast egress or ingress NetFlow accounting on an interface, use the **ip multicast netflow** command. To disable multicast NetFlow accounting, use the **no** form of this command.

**ip multicast netflow** { egress | ingress }

**no ip multicast netflow** { egress | ingress }

## Syntax Description

<b>egress</b>	Specifies multicast egress NetFlow accounting.
<b>ingress</b>	Specifies multicast ingress NetFlow accounting.

## Defaults

The defaults are as follows:

- Multicast egress NetFlow accounting is disabled.
- Multicast ingress NetFlow accounting is enabled

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

The output of the **show running-config** command does not indicate when multicast ingress accounting is enabled (but it does indicate when multicast ingress NetFlow accounting is disabled).

You must enable multicast egress NetFlow accounting on all interfaces for which you want to count outgoing multicast stream.

To display the multicast entries, enter the **show mls netflow ip** command.

## Examples

This example shows how to enable multicast ingress NetFlow accounting on the ingress Ethernet 1/0 interface:

```
Router# configure terminal
Router(config)# interface ethernet 1/0
Router(config-if)# ip multicast netflow ingress
Router(config-if)# end
```

## Related Commands

Command	Description
<b>ip multicast netflow rpf-failure</b>	Enables NetFlow accounting for multicast data that fails the RPF check.
<b>show ip flow interfaces</b>	Displays NetFlow accounting configuration on interfaces.

## ip multicast route-limit

To limit the number of multicast routes (mroutes) that can be added to a multicast routing table, use the **ip multicast route-limit** command. To disable this configuration, use the **no** form of this command.

```
ip multicast [vrf vrf-name] route-limit limit [threshold]
```

```
no ip multicast [vrf vrf-name] route-limit limit [threshold]
```

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
<i>limit</i>	Number of mroutes that can be added; valid values are from 1 to 2147483647.	
<i>threshold</i>	(Optional) Number of mroutes that cause a warning message to occur; valid values are from 1 to 2147483647.	

**Defaults** *limit* is 2147483647.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **ip multicast route-limit** command limits the number of multicast routes that can be added to a router and generates an error message when the limit is exceeded. If you set the *threshold* argument, a threshold error message is generated when the threshold is exceeded, and the message continues to occur until the number of mroutes reaches the limit set by the *limit* argument.

The mroute warning *threshold* must not exceed the mroute *limit*.

**Examples** This example shows how to set the mroute limit at 200,000 and the threshold at 20,000 for a VRF instance named cisco:

```
Router(config)# ip multicast vrf cisco route-limit 200000 20000
Router(config)#
```

# ip multicast-routing

To enable IP multicast routing, use the **ip multicast-routing** command. To disable IP multicast routing, use the **no** form of this command.

**ip multicast-routing** [*vrf vrf-name*] [**distributed**]

**no ip multicast-routing** [*vrf vrf-name*]

Syntax Description		
	<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
	<b>distributed</b>	(Optional) Enables MDS.

**Defaults** This command is disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** When IP multicast routing is disabled, no multicast packets are forwarded.

**Examples** This example shows how to enable IP multicast routing:

```
Router(config)# ip multicast-routing
Router(config)#
```

This example shows how to enable IP multicast routing on a specific VRF:

```
Router(config)# ip multicast-routing vrf vrf1
Router(config)#
```

This example shows how to disable IP multicast routing:

```
Router(config)# no ip multicast-routing
Router(config)#
```

Related Commands	Command	Description
	<b>ip pim</b>	Enables PIM on an interface.

## ip multicast rpf backoff

To set the PIM-backoff interval, use the **ip multicast rpf backoff** command. To return to the default settings, use the **no** form of this command.

**ip multicast rpf backoff** *{ {min max} | disable }*

**no ip multicast rpf backoff**

Syntax Description		
<i>min</i>	Initial RPF-backoff delay in milliseconds; valid values are from 1 to 65535 milliseconds.	
<i>max</i>	Maximum RPF-backoff delay in milliseconds; valid values are from 1 to 65535 milliseconds.	
<b>disable</b>	Disables the triggered RPF check.	

### Defaults

If you enable the triggered RPF check, the defaults are as follows:

- *min* is **500** milliseconds.
- *max* is **5000** milliseconds.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

If you do not enable the triggered RPF check, PIM periodically polls the routing tables for changes (set using the **ip multicast rpf interval** command). When you enable the triggered RPF check, PIM polls the routing tables when a change in the routing tables occurs. The *min* argument sets the initial backoff time. Once triggered, PIM waits for additional routing table changes. If the *min* period expires without further routing table changes, PIM scans for routing changes. If additional routing changes occur during the backoff period, PIM doubles the length of the backoff period. You can set the maximum interval for the doubled backoff period with the *max* argument.

Use this command in the following situation:

- You have frequent route changes in your device (for example, on a dial-in router).
- You want to either reduce the maximum RPF-check interval for faster availability of IP multicast on newly established routes, or you want to increase the RPF-check interval to reduce the CPU load that is introduced by the RPF check.

---

**Examples**

This example shows how to set the PIM-backoff interval in milliseconds:

```
Router(config)# ip multicast rpf backoff 100
Router(config)#
```

---

**Related Commands**

Command	Description
<a href="#">ip multicast rpf interval</a>	Sets the RPF consistency-check interval.
<a href="#">show ip rpf events</a>	Displays the triggered RPF statistics.

# ip multicast rpf interval

To set the RPF consistency-check interval, use the **ip multicast rpf interval** command. To return to the default settings, use the **no** form of this command.

**ip multicast rpf interval** *interval*

**no ip multicast rpf interval**

<b>Syntax Description</b>	<i>interval</i>	Interval in seconds between RPF checks; valid values are from 1 to 10 seconds.
---------------------------	-----------------	--

<b>Defaults</b>	10 seconds
-----------------	------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	The <b>ip multicast rpf interval</b> command sets the interval PIM and polls the routing tables for changes.
-------------------------	--

**Examples** This example shows how to set the RPF consistency-check interval in seconds:

```
Router(config)# ip multicast rpf interval 5
Router(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ip multicast rpf backoff</b>	Sets the PIM-backoff interval.

# ip pim accept-register

To configure a candidate rendezvous-point router to filter PIM register messages, use the **ip pim accept-register** command. To disable this function, use the **no** form of this command.

```
ip pim [vrf vrf-name] accept-register {list access-list | route-map map-name}
```

```
no ip pim [vrf vrf-name] accept-register {list access-list | route-map map-name}
```

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
<b>list</b> <i>access-list</i>	Specifies the extended access-list number or name.	
<b>route-map</b> <i>map-name</i>	Specifies the route-map name.	

Defaults	Disabled
----------	----------

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Usage Guidelines	Use this command to prevent unauthorized sources from registering with the rendezvous point. If an unauthorized source sends a register message to the rendezvous point, the rendezvous point immediately sends a register-stop message.
------------------	--

Examples	This example shows how to restrict the rendezvous point from allowing sources in the SSM range of addresses to register with the rendezvous point. These statements need to be configured only on the rendezvous point.
----------	---

```
Router(config)# ip pim accept-register list no-ssm-range
Router(config)# ip access-list extended no-ssm-range
   deny ip any 232.0.0.0 0.255.255.255
   permit ip any any
Router(config)#
```

## ip pim accept-rp

To configure a router to accept join or prune messages that are destined for a specified rendezvous point and for a specific list of groups, use the **ip pim accept-rp** command. To remove the check, use the **no** form of this command.

```
ip pim [vrf vrf-name] accept-rp {rp-address | auto-rp} [access-list]
```

```
no ip pim [vrf vrf-name] accept-rp {rp-address | auto-rp} [access-list]
```

### Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
<i>rp-address</i>	Address of the rendezvous point that is allowed to send join messages to groups in the range specified by the group access list.
<b>auto-rp</b>	Specifies that join and register messages are accepted only for rendezvous points that are in the Auto-RP cache.
<i>access-list</i>	(Optional) Access-list number or name that defines which groups are subject to the check.

### Defaults

Disabled—All join messages and prune messages are processed.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

This command causes the router to accept only (\*, G) join messages that are destined for the specified rendezvous-point address. Additionally, the group address must be in the range specified by the access list.

When the *rp-address* argument is one of the addresses of the system, the system is the rendezvous point only for the specified group range specified by the access list. When the group address is not in the group range, the rendezvous point does not accept join or register messages and responds immediately to register messages with register-stop messages.

### Examples

This example shows how to configure the router to accept join or prune messages that are destined for the rendezvous point at address 172.17.1.1 for the multicast group 224.2.2.2:

```
Router(config)# ip pim accept-rp 172.17.1.1 3
access-list 3 permit 224.2.2.2
```

Related Commands	Command	Description
	<b>access-list (IP standard)</b>	Defines a standard IP access list.

## ip pim bidir-enable

To enable bidir-PIM, use the **ip pim bidir-enable** command. To disable bidir-PIM, use the **no** form of this command.

**ip pim [vrf vrf-name] bidir-enable**

**no ip pim [vrf vrf-name] bidir-enable**

Syntax Description	<b>vrf vrf-name</b> (Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.				
Defaults	Disabled				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Release</th> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border-bottom: 1px solid black;">12.2(18)ZY</td> <td style="border-bottom: 1px solid black;">Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)ZY	Support for this command was introduced.
Release	Modification				
12.2(18)ZY	Support for this command was introduced.				

Usage Guidelines	<p>When bidir-PIM is disabled, the switch operates similarly to a router without bidir-PIM support. The following conditions apply:</p> <ul style="list-style-type: none"> <li>• PIM hello messages that are sent by the router do not contain the bidirectional mode option.</li> <li>• The router does not send designated forwarder election messages and ignores designated forwarder election messages that are received.</li> <li>• The <b>ip pim rp-address</b>, <b>ip pim send-rp-announce</b>, and <b>ip pim rp-candidate</b> commands are treated as follows: <ul style="list-style-type: none"> <li>– If these commands are configured when bidir-PIM is disabled, bidirectional mode is not a configuration option.</li> <li>– If these commands are configured with the bidirectional mode option when bidir-PIM is enabled and then bidir-PIM is disabled, these commands are removed from the CLI. You must enter these commands again with the bidirectional-mode option when you reenables bidir-PIM.</li> </ul> </li> <li>• The <b>df</b> keyword for the <b>show ip pim interface</b> command is not supported.</li> </ul>
------------------	---

**Examples** This example shows how to enable bidir-PIM:

```
Router(config)# ip pim bidir-enable
Router(config)#
```

This example shows how to disable bidir-PIM:

```
Router(config)# no ip pim bidir-enable
Router(config)#
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ip pim rp-address</b>	Configures the address of a PIM rendezvous point for a particular group.
<b>ip pim rp-candidate</b>	Configures the router to advertise itself as a PIM Version 2 rendezvous-point candidate to the BSR.
<b>ip pim send-rp-announce</b>	Uses Auto-RP to configure groups for which the router acts as a rendezvous point.

## ip pim bsr-candidate

To configure the router to announce its candidacy as a BSR, use the **ip pim bsr-candidate** command. To remove this router as a candidate bootstrap router, use the **no** form of this command.

**ip pim** [**vrf** *vrf-name*] **bsr-candidate** *interface-type interface-number* [*hash-mask-length*] [*priority*]

**no ip pim** [**vrf** *vrf-name*] **bsr-candidate**

### Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
<i>interface-type</i> <i>interface-number</i>	Interface type and number on this router from which the BSR address is derived to make it a candidate.
<i>hash-mask-length</i>	(Optional) Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called.
<i>priority</i>	(Optional) BSR priority; valid values are from 0 to 255.

### Defaults

The default settings are as follows:

- Disabled.
- If enabled, the *priority* is **0**.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

This command causes the router to send bootstrap messages to all its PIM neighbors with the address of the designated interface as the BSR address. Each neighbor compares the BSR address with the address it had from previous bootstrap messages (not necessarily received on the same interface). If the current address is the same or higher address, it caches the current address and forwards the bootstrap message. Otherwise, the router drops the bootstrap message.

This router continues to be the BSR until it receives a bootstrap message from another candidate BSR saying that it has a higher priority (or if the same priority, a higher IP address).

Use this command only in backbone routers that have good connectivity to all parts of the PIM domain. A stub router that relies on an on-demand dialup link to connect to the rest of the PIM domain is not a good BSR candidate.

You must enable the *interface-type* with PIM.

When setting the *hash-mask-length* argument, all groups with the same seed hash correspond to the same rendezvous point. For example, if this value is 24, only the first 24 bits of the group addresses are applicable; using this setting allows you to get one rendezvous point for multiple groups.

When setting the *priority*, the BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IP address is the BSR.

### Examples

This example shows how to configure the IP address of the router on Ethernet interface 0 to be a candidate BSR with a priority of 10:

```
Router(config)# ip pim bsr-candidate ethernet 0 10
Router(config)#
```

### Related Commands

Command	Description
<b>ip pim bsr border</b>	Prevents BSR messages from being sent or received through an interface.
<b>ip pim rp-candidate</b>	Configures the router to advertise itself as a PIM Version 2 rendezvous-point candidate to the BSR.
<b>ip pim send-rp-discovery</b>	Configures the router as a rendezvous-point mapping agent.
<b>show ip pim bsr</b>	Displays the BSR information.
<b>show ip pim rp</b>	Displays active rendezvous points that are cached with associated multicast routing entries.

## ip pim register-rate-limit

To set a limit on the maximum number of PIM-SM register messages that are sent per second for each (S,G) routing entry, use the **ip pim register-rate-limit** command. To disable this limit, use the **no** form of this command.

```
ip pim [vrf vrf-name] register-rate-limit rate
```

```
no ip pim [vrf vrf-name] register-rate-limit
```

<b>Syntax Description</b>	<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
	<i>rate</i>	Maximum number of register messages that are sent per second by the router; valid values are from 1 to 65535 messages per second.

**Defaults** No limit is defined.

**Command Modes** Global configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Use this command to limit the number of register messages that the designated router allows for each (S,G) entry. Enabling this command limits the load on the designated router and rendezvous point but drops those register messages that exceed the set limit. Receivers may experience data packet loss within the first second in which register messages are sent from bursty sources.

If you enter the **ip pim dense-mode proxy-register** command, then you must enter the **ip pim register-rate-limit** command because of the potentially large number of sources from the dense-mode area that may send data into the sparse-mode region (and need registering in the border router).

This command applies only to sparse mode (S,G) multicast routing entries.

**Examples** This example shows how to set a limit on PIM-SM register messages with a maximum rate of two register messages per second:

```
Router(config)# ip pim register-rate-limit 2
Router(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ip pim</b>	Enables PIM on an interface.

## ip pim register-source

To configure the IP source address of a register message to an interface address other than the outgoing interface address of the designated router leading toward the rendezvous point, use the **ip pim register-source** command. To disable this configuration, use the **no** form of this command.

```
ip pim [vrf vrf-name] register-source interface-type interface-number
```

```
no ip pim [vrf vrf-name] register-source
```

### Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
<i>interface-type</i> <i>interface-number</i>	Interface type and interface number that identify the IP source address of a register message.

### Defaults

The IP address of the outgoing interface of the designated router leading toward the rendezvous point is used as the IP source address of a register message.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

This command is required only when the IP source address of a register message is not a uniquely routed address to which the rendezvous point can send packets. This situation may occur if the source address is filtered so that packets sent to it are not forwarded or if the source address is not unique to the network. In these cases, the replies sent from the rendezvous point to the source address fail to reach the designated router and result in PIM-SM protocol failures.

If you do not configure an IP source address or if the configured source address is not in service, the IP address of the outgoing interface of the designated router leading to the rendezvous point is used as the IP source address of the register message. We recommend that you use a loopback interface with an IP address that is uniquely routed throughout the PIM-SM domain.

### Examples

This example shows how to configure the IP source address of the register message to the loopback 3 interface of a designated router:

```
Router(config)# ip pim register-source loopback 3
Router(config)#
```

## ip pim rp-announce-filter

To filter incoming Auto-RP announcement messages coming from the rendezvous point, use the **ip pim rp-announce-filter** command. To remove the filter, use the **no** form of this command.

```
ip pim [vrf vrf-name] rp-announce-filter rp-list access-list group-list access-list
```

```
no ip pim [vrf vrf-name] rp-announce-filter rp-list access-list group-list access-list
```

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
<b>rp-list</b> <i>access-list</i>	Specifies the number or name of a standard access list of rendezvous-point addresses that are allowable for the group ranges supplied in the <b>group-list</b> <i>access-list</i> combination.	
<b>group-list</b> <i>access-list</i>	Specifies the number or name of a standard access list that describes the multicast groups that the RPs serve.	

**Defaults** All rendezvous-point announcements are accepted.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Configure this command on the PIM rendezvous-point mapping agent. We recommend that if you use more than one rendezvous-point mapping agent, make the filters among them consistent so that there are no conflicts in the mapping state when the announcing agent is removed.

**Examples** This example shows how to configure the router to accept rendezvous-point announcements from rendezvous points in access list 1 for group ranges that are described in access list 2:

```
Router(config)# ip pim rp-announce-filter rp-list 1 group-list 2
Router(config)#
```

Related Commands	Command	Description
	<b>access-list (IP standard)</b>	Defines a standard IP access list.

## ip pim rp-candidate

To configure the router to advertise itself as a PIM Version 2 rendezvous-point candidate to the BSR, use the **ip pim rp-candidate** command. To remove this router as a rendezvous-point candidate, use the **no** form of this command.

```
ip pim [vrf vrf-name] rp-candidate interface-type interface-number [group-list access-list]
[bidir]
```

```
no ip pim [vrf vrf-name] rp-candidate
```

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
<i>interface-type</i> <i>interface-number</i>	IP address associated with this interface type and number is advertised as a candidate rendezvous-point address.	
<b>group-list</b> <i>access-list</i>	(Optional) Specifies the standard IP access-list number or name that defines the group prefixes that are advertised with the rendezvous-point address.	
<b>bidir</b>	(Optional) Indicates that the multicast groups that are specified by the <i>access-list</i> argument operate in bidirectional mode.	

Defaults	Disabled
----------	----------

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command causes the router to send a PIM Version 2 message advertising itself as a rendezvous-point candidate to the BSR. The addresses allowed by the access list, together with the router identified by the type and number, constitute the rendezvous point and its range of addresses for which it is responsible.

Use this command only in backbone routers that have good connectivity to all parts of the PIM domain. A stub router that relies on an on-demand dialup link to connect to the rest of the PIM domain is not a good rendezvous-point candidate.

Use this command with the **bidir** keyword when you want bidirectional forwarding and you are using the PIM Version 2 BSR mechanism to distribute group-to-rendezvous point mappings. Other options are as follows:

- If you are using Auto-RP to distribute group-to-rendezvous point mappings, use the **bidir** keyword with the **ip pim send-rp-announce** command.
- If you are not distributing group-to-rendezvous point mappings using either Auto-RP or the PIM Version 2 BSR mechanism, use the **bidir** keyword with the **ip pim rp-address** command.

The *access-list* name cannot contain a space or quotation mark and must begin with an alphabetic character to avoid confusion with numbered access lists.

If you enter this command without the **bidir** keyword, the groups that are specified operate in PIM sparse mode.

### Examples

This example shows how to configure the router to advertise itself as a rendezvous-point candidate to the BSR in its PIM domain. Standard access-list number 4 specifies the group prefix that is associated with the rendezvous point that has the address identified by Ethernet interface 2. That rendezvous point is responsible for the groups with the prefix 239.

```
Router(config)# ip pim rp-candidate 192.168.37.33 ethernet 2 group-list 4
access-list 4 permit 239.0.0.0 0.255.255.255
Router(config)#
```

### Related Commands

Command	Description
<a href="#">ip pim bsr-candidate</a>	Configures the router to announce its candidacy as a BSR.
<a href="#">ip pim rp-announce-filter</a>	Filters incoming Auto-RP announcement messages coming from the rendezvous point.
<a href="#">ip pim send-rp-announce</a>	Uses Auto-RP to configure groups for which the router acts as a rendezvous point.

## ip pim send-rp-announce

To use Auto-RP to configure groups for which the router will act as a rendezvous point, use the **ip pim send-rp-announce** command. To deconfigure this router as a rendezvous point, use the **no** form of this command.

```
ip pim [vrf vrf-name] send-rp-announce interface-type interface-number scope ttl-value
[group-list access-list] [interval seconds] [bidir]
```

```
no ip pim [vrf vrf-name] send-rp-announce
```

Syntax	Description
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
<i>interface-type</i> <i>interface-number</i>	Interface type and number that is used to define the rendezvous-point address.
<b>scope</b> <i>ttl-value</i>	Time-to-live (TTL) value that limits the number of Auto-RP announcements; valid values are from 1 to 255.
<b>group-list</b> <i>access-list</i>	(Optional) Specifies the standard IP access-list number or name that defines the group prefixes that are advertised in association with the rendezvous-point address.
<b>interval</b> <i>seconds</i>	(Optional) Specifies the interval between rendezvous-point announcements in seconds; valid values are from 1 to 16383 seconds.
<b>bidir</b>	(Optional) Indicates that the multicast groups that are specified by the <i>access-list</i> argument operate in bidirectional mode.

### Defaults

The default settings are as follows:

- Auto-RP is disabled.
- If enabled, the *seconds* is 60 seconds.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

Use this command in the router that you want as a rendezvous point. When you are using Auto-RP to distribute group-to-rendezvous point mappings, this command causes the router to send an Auto-RP announcement message to the well-known group CISCO-RP-ANNOUNCE (224.0.1.39). This message announces the router as a rendezvous-point candidate for the groups in the range that are described by the access list.

Use this command with the **bidir** keyword when you want bidirectional forwarding and you are using Auto-RP to distribute group-to-rendezvous point mappings. Other options are as follows:

- If you are using the PIM Version 2 bootstrap router (PIMv2 BSR) mechanism to distribute group-to-rendezvous point mappings, use the **bidir** keyword with the **ip pim rp-candidate** command.
- If you are not distributing group-to-rendezvous point mappings using either Auto-RP or the PIMv2 BSR mechanism, use the **bidir** keyword with the **ip pim rp-address** command.

If you enter this command without the **bidir** keyword, the specified groups operate in PIM-SM.

The *access-list* name cannot contain a space or quotation mark and must begin with an alphabetic character to avoid confusion with numbered access lists.

The total holdtime of the rendezvous-point announcements is automatically set to three times the value of the interval.

### Examples

This example shows how to send rendezvous-point announcements out all PIM-enabled interfaces for a maximum of 31 hops. The IP address by which the router wants to be identified as a rendezvous point is the IP address that is associated with Ethernet interface 0. Access list 5 describes the groups for which this router serves as a rendezvous point.

```
Router(config)# ip pim send-rp-announce ethernet0 scope 31 group-list 5
access-list 5 permit 224.0.0.0 15.255.255.255
```

### Related Commands

Command	Description
<b>access-list (IP standard)</b>	Defines a standard IP access list.
<b>ip pim rp-address</b>	Configures the address of a PIM rendezvous point for a particular group.
<b>ip pim rp-candidate</b>	Configures the router to advertise itself as a PIM Version 2 rendezvous-point candidate to the BSR.

## ip pim send-rp-discovery

To configure the router as a rendezvous-point mapping agent, use the **ip pim send-rp-discovery** command. To restore the default value, use the **no** form of this command.

**ip pim** [**vrf** *vrf-name*] **send-rp-discovery** [*interface-type interface-number*] **scope** *ttl-value*

**no ip pim** [**vrf** *vrf-name*] **send-rp-discovery**

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
<i>interface-type</i> <i>interface-number</i>	(Optional) Interface type and number that is used to define the rendezvous-point mapping agent address.	
<b>scope</b> <i>ttl-value</i>	Specifies the time-to-live (TTL) value in the IP header that keeps the discovery messages within this number of hops; valid values are from 1 to 255.	

**Defaults** The router is not a rendezvous-point mapping agent.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Configure this command on the router that is designated as a rendezvous-point mapping agent. Specify a TTL large enough to cover your PIM domain.

When Auto-RP is used, the following occurs:

1. The rendezvous-point mapping agent listens on well-known group address CISCO-RP-ANNOUNCE (224.0.1.39), to which rendezvous-point candidates send.
2. The rendezvous-point mapping agent sends rendezvous point-to-group mappings in an Auto-RP rendezvous point discovery message to the well-known group CISCO-RP-DISCOVERY (224.0.1.40). The TTL value limits how many hops that the message can take.
3. PIM-designated routers listen to this group and use the rendezvous points that they learn about from the discovery message.

**Examples** This example shows how to limit Auto-RP rendezvous-point discovery messages to 20 hops:

```
Router(config)# ip pim send-rp-discovery scope 20
Router(config)#
```

## ip pim snooping (global configuration mode)

To enable PIM snooping globally, use the **ip pim snooping** command. To disable PIM snooping globally, use the **no** form of this command.

**ip pim snooping**

**no ip pim snooping**

---

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

---

**Defaults** Disabled

---

**Command Modes** Global configuration

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Usage Guidelines** PIM snooping is not supported on groups that are connected to the reserved MAC address range (for example, 0100.5e00.00xx).

When you disable PIM snooping globally, PIM snooping is disabled on all VLANs.

---

**Examples** This example shows how to enable PIM snooping globally:

```
Router(config)# ip pim snooping
Router(config)#
```

This example shows how to disable PIM snooping globally:

```
Router(config)# no ip pim snooping
Router(config)#
```

---

Related Commands	Command	Description
	<a href="#">show ip pim snooping</a>	Displays the information about IP PIM snooping.

---

# ip pim snooping (interface configuration mode)

To enable PIM snooping on an interface, use the **ip pim snooping** command. To disable PIM snooping on an interface, use the **no** form of this command.

**ip pim snooping**

**no ip pim snooping**

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

**Defaults** Disabled

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** PIM snooping is not supported on groups that are connected to the reserved MAC address range (for example, 0100.5e00.00xx).

You must enable PIM snooping globally before enabling PIM snooping on an interface. When you disable PIM snooping globally, PIM snooping is disabled on all VLANs.

You can enable PIM snooping on VLAN interfaces only.

**Examples** This example shows how to enable PIM snooping on a VLAN interface:

```
Router(config)# interface vlan 101
Router(config-if)# ip pim snooping
Router(config-f)#
```

This example shows how to disable PIM snooping on a VLAN interface:

```
Router(config-if)# no ip pim snooping
Router(config-f)#
```

Related Commands	Command	Description
	<a href="#">show ip pim snooping</a>	Displays information about IP PIM snooping.

## ip pim snooping dr-flood

To enable flooding of the packets to the designated router, use the **ip pim snooping dr-flood** command. To disable the flooding of the packets to the designated router, use the **no** form of this command.

**ip pim snooping dr-flood**

**no ip pim snooping dr-flood**

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

**Defaults** Enabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** PIM snooping is not supported on groups that are connected to the reserved MAC address range (for example, 0100.5e00.00xx).

Enter the **no ip pim snooping dr-flood** command only on switches that have no designated routers attached.

The designated router is programmed automatically in the (S,G) O-list.

**Examples** This example shows how to enable flooding of the packets to the designated router:

```
Router(config)# ip pim snooping dr-flood
Router(config)#
```

This example shows how to disable flooding of the packets to the designated router:

```
Router(config)# no ip pim snooping dr-flood
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show ip pim snooping</a>	Displays information about IP PIM snooping.

# ip pim spt-threshold

To configure when a PIM leaf router should join the shortest path source tree for the specified group, use the **ip pim spt-threshold** command. To restore the default value, use the **no** form of this command.

```
ip pim [vrf vrf-name] spt-threshold {kpbs | infinity} [group-list access-list]
```

```
no ip pim [vrf vrf-name] spt-threshold
```

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
<i>kpbs</i>	Traffic rate; valid values are from 0 to 4294967 kbps.	
<b>infinity</b>	Causes all sources for the specified group to use the shared tree.	
<b>group-list</b> <i>access-list</i>	(Optional) Specifies the groups to which the threshold applies.	

**Defaults** When this command is not used, the PIM leaf router joins the shortest path tree immediately after the first packet arrives from a new source.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** If a source sends at a rate greater than or equal to the traffic rate (the *kpbs* value), a PIM join message is triggered to construct a source tree.

The **group-list** *access-list* must be an IP standard access-list number or name. If the value is 0 or is omitted, the threshold applies to all groups.

If you specify the **infinity** keyword, all sources for the specified group use the shared tree. Specifying a group list access list indicates the groups to which the threshold applies.

If the traffic rate from the source drops below the threshold traffic rate, the leaf router will, after some amount of time, switch back to the shared tree and send a prune message to the source.

**Examples** This example shows how to set a threshold of 4 kbps. If the traffic rate goes above this threshold, the traffic to a group from a source causes the router to switch to the shortest path tree to that source:

```
Router(config)# ip pim spt-threshold 4
Router(config)#
```

## ip pim ssm

To define the SSM range of IP multicast addresses, use the **ip pim ssm** command. To disable the SSM range, use the **no** form of this command.

```
ip pim [vrf vrf-name] ssm {default | range access-list}
```

```
no ip pim [vrf vrf-name] ssm
```

Syntax Description	Parameter	Description
	<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
	<b>default</b>	Defines the SSM range access list as 232/8.
	<b>range</b> <i>access-list</i>	Specifies the standard IP access-list number or name defining the SSM range.

Defaults	Disabled
----------	----------

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Usage Guidelines	When an SSM range of IP multicast addresses is defined by the <b>ip pim ssm</b> command, no MSDP source-active messages are accepted or originated in the SSM range.
------------------	--

Examples	This example shows how to configure the SSM service for the IP address range that is defined by access list 4:
----------	--

```
access-list 4 permit 5541514541444
Router(config)# ip pim ssm range 4
```

Related Commands	Command	Description
	<b>ip igmp v3lite</b>	Enables acceptance and processing of IGMP v3lite membership reports on an interface.
	<b>ip urd</b>	Enables interception of TCP packets sent to the reserved URD port 465 on an interface and processing of URD channel subscription reports.

# ip pim state-refresh disable

To disable the processing and forwarding of PIM dense-mode refresh-control messages on a PIM router, use the **ip pim state-refresh disable** command. To reenble the processing and forwarding of PIM dense-mode refresh-control messages, use the **no** form of this command.

**ip pim** [*vrf vrf-name*] **state-refresh disable**

**no ip pim** [*vrf vrf-name*] **state-refresh disable**

## Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
----------------------------	--

## Defaults

The processing and forwarding of PIM dense-mode refresh-control messages is enabled on PIM routers that are running a Cisco IOS software release that supports the PIM dense-mode refresh-control feature.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

Configuring this command removes PIM dense-mode refresh-control information from PIM hello messages.

## Examples

This example shows how to disable the periodic forwarding of the PIM dense-mode refresh-control message down a source-based IP multicast distribution tree:

```
Router(config)# ip pim state-refresh disable
Router(config)#
```

## Related Commands

Command	Description
<b>ip pim state-refresh origination-interval</b>	Configures the origination of and the interval for PIM dense-mode state refresh-control messages on a PIM router.
<b>show ip pim interface</b>	Displays information about interfaces configured for PIM.
<b>show ip pim neighbor</b>	Displays the list that the PIM neighbors discovered.

# ip rgmp

To enable RGMP on an interface, use the **ip rgmp** command. To disable RGMP, use the **no** form of this command.

**ip rgmp**

**no ip rgmp**

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

**Defaults** The defaults are as follows:

- Enabled on Layer 2 interfaces (not configurable)
- Disabled on Layer 3 interfaces

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** These restrictions apply to RGMP on the PISA:

- You can enable RGMP on interfaces that are configured to support multicast routing.
- You must enable IGMP snooping on the Catalyst 6500 series switch.
- You must enable PIM on the Catalyst 6500 series switch.
- RGMP supports PIM sparse mode only. RGMP does not support PIM dense mode. RGMP explicitly supports the two AutoRP groups in dense mode by not restricting traffic to those groups but by flooding it to all router ports. For this reason, you should configure PIM sparse-dense mode. If you configure groups other than the AutoRP groups for dense mode, their traffic will not be correctly forwarded through router ports that have been enabled for RGMP.
- To effectively constrain multicast traffic with RGMP, connect RGMP-enabled routers to separate ports on RGMP-enabled Catalyst 6500 series switches.
- RGMP constrains only the traffic that exits through ports on which it detects an RGMP-enabled router. If a non-RGMP enabled router is detected on a port, that port receives all multicast traffic.
- RGMP does not support directly connected sources in the network. A directly connected source sends traffic into the network without signaling this information through RGMP or PIM. This traffic is not received by an RGMP-enabled router unless the router already requested receipt of that group through RGMP. This restriction applies to hosts and to functions in routers that source multicast traffic, such as the **ping** and **mtrace** commands, and multicast applications that source multicast traffic such as UDPTN.

- RGMP supports directly connected receivers in the network. Traffic to these receivers is restricted by IGMP snooping, or if the receiver is a router itself, by PIM and RGMP. CGMP is not supported in networks where RGMP is enabled on routers.
- Enabling RGMP and CGMP on a router interface is mutually exclusive. If RGMP is enabled on an interface, CGMP is silently disabled or vice versa.

---

**Examples**

This example shows how to enable RGMP:

```
Router(config-if)# ip rgmp
Router(config-if)#
```

This example shows how to disable RGMP:

```
Router(config-if)# no ip rgmp
Router(config-if)#
```

---

**Related Commands**

Command	Description
<a href="#">show running-config</a>	Displays the status and configuration of the module or Layer 2 VLAN.

# ip route-cache flow

To enable NetFlow switching for IP routing, use the **ip route-cache flow** command. To disable NetFlow switching, use the **no** form of this command.

**ip route-cache flow**

**no ip route-cache flow**

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

**Defaults** Disabled

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** NetFlow switching captures a set of traffic statistics as part of its switching function. These traffic statistics include user, protocol, port, and type of service information that can be used for network analysis and planning, accounting, and billing. To export NetFlow data, use the **ip flow-export destination** or the **ip flow-export source** command in the global configuration mode.

NetFlow switching is supported on IP and IP-encapsulated traffic over all interface types and encapsulations except for ISL/VLAN, ATM, Frame Relay interfaces when more than one input access control list is used on the interface, and ATM LANE.

For additional information on NetFlow switching, refer to the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*.



**Note**

NetFlow does consume additional memory and CPU resources compared to other switching modes; we recommend that you understand the resources that are required on your router before you enable NetFlow.

**Examples** This example shows how to enable NetFlow switching on the interface:

```
Router(config-if)# ip route-cache flow
Router(config-if)#
```

This example shows how to return the interface to its defaults (fast switching enabled; autonomous switching disabled):

```
Router(config-if)# no ip route-cache flow
Router(config-if)#
```

Related Commands	Command	Description
	<a href="#">ip flow-export destination</a>	Exports the NetFlow cache entries to a specific destination.
	<a href="#">show ip cache flow</a>	Displays a summary of the NetFlow cache-flow entries.

## ip sticky-arp (global configuration)

To enable sticky ARP, use the **ip sticky-arp** command. To disable sticky ARP, use the **no** form of this command.

**ip sticky-arp**

**no ip sticky-arp**

---

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

---

**Defaults** Enabled

---

**Command Modes** Global configuration

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Usage Guidelines** You can enter the **ip sticky-arp (interface configuration)** command to disable sticky ARP on a specific interface.

ARP entries that are learned on Layer 3 interfaces are sticky ARP entries. We recommend that you display and verify ARP entries on the Layer 3 interface using the **show arp** command.

For security reasons, sticky ARP entries on the Layer 3 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 Layer 3 interface do not age out, you must manually remove ARP entries on the Layer 3 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:

```
Router(config) ip sticky-arp
Router(config)
```

This example shows how to disable sticky ARP:

```
Router(config) no ip sticky-arp
Router(config)
```

---

**Related Commands**

Command	Description
<b>arp</b>	Enables ARP entries for static routing over the SMDS network.
<b>ip sticky-arp (interface configuration)</b>	Enables sticky ARP on an interface.
<b>show arp</b>	Displays the ARP table.

## ip sticky-arp (interface configuration)

To enable sticky ARP on an interface, use the **ip sticky-arp** command. To remove the command, use the **no** form of this command.

**ip sticky-arp [ignore]**

**no ip sticky-arp [ignore]**

<b>Syntax Description</b>	<b>ignore</b> (Optional) Overwrites the <b>ip sticky-arp (global configuration)</b> command.
---------------------------	--

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	<p>You can enter this command on any Layer 3 interface.</p> <p>You can enter the <b>ip sticky-arp ignore</b> command to overwrite the PVLAN sticky-ARP global configuration on a specific interface.</p>
-------------------------	--

<b>Examples</b>	This example shows how to enable sticky ARP on an interface:
-----------------	--

```
Router(config-if) ip sticky-arp
Router(config-if)
```

This example shows how to remove the previously configured command on an interface:

```
Router(config-if) no ip sticky-arp
Router(config-if)
```

This example shows how to disable sticky ARP on an interface:

```
Router(config-if) ip sticky-arp ignore
Router(config-if)
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>arp</b>	Enables ARP entries for static routing over the SMDS network.
	<b>ip sticky-arp (global configuration)</b>	Enables sticky ARP.
	<b>show arp</b>	Displays the ARP table.

# ip unnumbered

To enable IP processing on a serial interface without assigning an explicit IP address to the interface, use the **ip unnumbered** command. To disable IP processing on the interface, use the **no** form of this command.

**ip unnumbered** *interface-type number*

**no ip unnumbered** *interface-type number*

Syntax Description	<i>interface-type number</i>
	Type and number of another interface on which the router has an assigned IP address; the interface cannot be another unnumbered interface.

Defaults	Disabled
----------	----------

Command Modes	Interface configuration or Ethernet VLAN subinterface
---------------	---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The interface that you specify by the *interface-type number* arguments must be enabled (listed as “up” in the **show interfaces** command display).

The unnumbered interfaces and subinterfaces support peer IP address allocation through DHCP and have DHCP option 82 support.

The following restrictions apply when using IP unnumbering:

- You cannot enable IP unnumbering for a range of interfaces or subinterfaces that are configured through an interface or a subinterface range configuration.
- You cannot use the **ping EXEC** command to determine whether the interface is up, because the interface has no address. You can use SNMP to monitor the interface status remotely.
- You cannot boot a runnable image over an unnumbered serial interface.
- You cannot support IP security options on an unnumbered interface.

**Examples** This example shows how to enable the IP unnumbered feature in the subinterface mode for Ethernet VLAN subinterfaces:

```
Router (config)# interface fastethernet1/0.1
Router (config-subif)# encapsulation dot1q 10
Router (config-subif)# ip unnumbered ethernet 3/0
```

This example shows how to disable the IP unnumbered feature for Ethernet physical interfaces:

```
Router (config)# interface fastethernet 1
Router (config-if)# no ip unnumbered loopback 0
```

■ ip unnumbered

```
Router (config-if)#
```

---

**Related Commands**

Command	Description
<b>show ipv6 mld snooping explicit-tracking vlan</b>	Displays MLDv2 snooping information.

---

# ipv6 mfib-cef

To enable CEF-based (interrupt level) IPv6 multicast forwarding for outgoing packets on a specific interface, use the **ipv6 mfib-cef** command. To disable CEF-based IPv6 multicast forwarding, use the **no** form of this command.

**ipv6 mfib-cef**

**no ipv6 mfib-cef**

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

**Defaults** Enabled

**Command Modes** Interface configuration

Release	Modification
12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** CEF-based (interrupt level) IPv6 multicast forwarding is enabled by default when you enable CEF-based IPv6 multicast routing.

Use the **show ipv6 mfib interface** command to display the multicast forwarding interface status.

**Examples** This example shows how to enable CEF-based IPv6 multicast forwarding:

```
Router(config-if) ipv6 mfib-cef
Router(config-if)
```

This example shows how to disable CEF-based IPv6 multicast forwarding:

```
Router(config-if) no ipv6 mfib-cef
Router(config-if)
```

Command	Description
<b>show ipv6 mfib interface</b>	Displays information about IPv6 multicast-enabled interfaces and their forwarding status.

## ipv6 mfib hardware-switching

To configure hardware switching for IPv6 multicast packets on a global basis, use the **ipv6 mfib hardware-switching** command. To return to the default settings, use the **no** form of this command.

**ipv6 mfib hardware-switching** [**connected** | {**replication-mode ingress**}]

**no ipv6 mfib hardware-switching** [**connected** | {**replication-mode ingress**}]

Syntax Description	connected	(Optional) Allows you to download the interface and mask entry.
	<b>replication-mode ingress</b>	(Optional) Sets the hardware replication mode to ingress.

### Defaults

The defaults are as follows:

- **connected**—Enabled; installs subnet entries in the ACL-TCAM.
- **replication-mode**—Automatically detected; but can be forced to ingress.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

You can use the **ipv6 mfib hardware-switching** command for PIM SSM and PIM Bidir to prevent installation of the subnet entries on a global basis.

### Examples

This example shows how to prevent the installation of the subnet entries on a global basis:

```
Router(config) ipv6 mfib hardware-switching
Router(config)
```

This example shows how to set the hardware replication mode to ingress:

```
Router(config) ipv6 mfib hardware-switching replication-mode
Router(config)
```

### Related Commands

Command	Description
<a href="#">show platform software ipv6-multicast</a>	Displays information about the platform software IPv6 multicast.

# ipv6 mld snooping

To enable the MLDv2 snooping globally, use the **ipv6 mld snooping** command. To disable the MLDv2 snooping globally, use the **no** form of this command.

**ipv6 mld snooping**

**no ipv6 mld snooping**

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

**Defaults** Enabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** To use MLDv2 snooping, configure a Layer 3 interface in the subnet for IPv6 multicast routing or enable the MLDv2 snooping querier in the subnet.

**Examples** This example shows how to enable MLDv2 snooping globally:

```
Router(config)# ipv6 mld snooping
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show ipv6 mld snooping</a>	Displays MLDv2 snooping information.

## ipv6 mld snooping explicit-tracking

To enable explicit host tracking, use the **ipv6 mld snooping explicit-tracking** command. To disable the explicit host tracking, use the **no** form of this command.

**ipv6 mld snooping explicit-tracking**

**no ipv6 mld snooping explicit-tracking**

---

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

---

**Defaults** Enabled

---

**Command Modes** Interface configuration

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Usage Guidelines** Explicit host tracking is supported only with MLDv2 hosts.

When you enable explicit host tracking and the Catalyst 6500 series switch is working in proxy-reporting mode, the router may not be able to track all the hosts that are behind a VLAN interface. In proxy-reporting mode, the Catalyst 6500 series switch forwards only the first report for a channel to the router and suppresses all other reports for the same channel.

With MLDv2 proxy reporting, the Catalyst 6500 series switch does proxy reporting for unsolicited reports and reports that are received in the general query interval.

Proxy reporting is turned on by default. When you disable proxy reporting, the Catalyst 6500 series switch works in transparent mode and updates the MLDv2 snooping database as it receives reports and forwards this information to the upstream router. The router can then explicitly track all reporting hosts.

Disabling explicit tracking disables fast-leave processing and proxy reporting.

MLDv2 supports explicit host tracking of membership information on any port. The explicit host-tracking database is used for fast-leave processing for MLDv2 hosts, proxy reporting, and statistics collection. When you enable explicit host tracking on a VLAN, the MLDv2 snooping software processes the MLDv2 report that it receives from a host and builds an explicit host-tracking database that contains the following information:

- The port that is connected to the host.
- The channels that are reported by the host.
- The filter mode for each group that are reported by the host.
- The list of sources for each group that are reported by the hosts.
- The router filter mode of each group.
- The list of hosts for each group that request the source.

---

**Examples**

This example shows how to enable explicit host tracking:

```
Router(config-if)# ipv6 mld snooping explicit-tracking
Router(config-if)#
```

---

**Related Commands**

Command	Description
<a href="#">ipv6 mld snooping limit</a>	Configures the MLDv2 limits.
<a href="#">show ipv6 mld snooping explicit-tracking</a>	Displays MLDv2 snooping information.

---

## ipv6 mld snooping last-member-query-interval

To configure the last member query interval for MLDv2 snooping, use the **ipv6 mld snooping last-member-query-interval** command. To return to the default settings, use the **no** form of this command.

**ipv6 mld snooping last-member-query-interval** *interval*

**no ipv6 mld snooping last-member-query-interval**

<b>Syntax Description</b>	<i>interval</i>	Interval for the last member query; valid values are from 100 to 900 milliseconds in multiples of 100 milliseconds.
---------------------------	-----------------	---

<b>Defaults</b>	1000 milliseconds (1 second); see the “Usage Guidelines” section for additional information.
-----------------	--

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** When a multicast host leaves a group, the host sends an MLDv2 leave. To check if this host is the last to leave the group, an MLDv2 query is sent out when the leave is seen and a timer is started. If no reports are received before the timer expires, the group record is deleted.

The *interval* is the actual time that the Catalyst 6500 series switch waits for a response for the group-specific query.

If you enter an interval that is not a multiple of 100, the interval is rounded to the next lowest multiple of 100. For example, if you enter 999, the interval is rounded down to 900 milliseconds.

If you enable MLDv2 fast-leave processing and you enter the **no ipv6 mld snooping last-member-query-interval** command, the interval is set to 0 seconds; fast-leave processing always assumes a higher priority.

Even though the valid interval range is 100 to 1000 milliseconds, you cannot enter a value of **1000**. If you want this value, you must enter the **no ipv6 mld snooping last-member-query-interval** command and return to the default value (1000 milliseconds).

---

**Examples**

This example shows how to configure the last-member-query-interval to 200 milliseconds:

```
Router(config-if)# ipv6 mld snooping last-member-query-interval 200
Router(config-if)#
```

---

**Related Commands**

Command	Description
<a href="#">show ipv6 mld snooping</a>	Displays MLDv2 snooping information.

---

## ipv6 mld snooping limit

To configure the MLDv2 limits, use the **ipv6 mld snooping limit** command. To return to the default settings, use the **no** form of this command.

```
ipv6 mld snooping limit {{12-entry-limit max-entries} | rate pps} | track max-entries}}
```

```
no ipv6 mld snooping limit {12-entry-limit | rate | track}
```

Syntax Description		
<b>12-entry-limit</b> <i>max-entries</i>	Specifies the maximum number of Layer 2 entries that can be installed by MLD snooping; valid values are from 1 to 100000 entries.	
<b>rate</b> <i>pps</i>	Specifies the rate limit of incoming MLDv2 messages; valid values are from 100 to 6000 packets per second.	
<b>track</b> <i>max-entries</i>	Specifies the maximum number of entries in the explicit-tracking database; valid values are from 0 to 128000 entries.	

**Defaults** *max-entries* is **32000**.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Each entry in the explicit-tracking database is identified by the source IP, group IP, port, VLAN, and reporter IP.

When you set the *max-entries* to **0**, explicit-tracking is disabled.

When the explicit-tracking database exceeds the configured *max-entries*, a syslog message is generated.

When you reduce the *max-entries*, the explicit-tracking database does not decrease in size immediately. The explicit-tracking database gradually shrinks as reporters time out.

**Examples** This example shows how to set the maximum number of Layer 2 entries that can be installed by MLD snooping:

```
Router(config)# ipv6 mld snooping limit 12-entry-limit 20000
Router(config)#
```

This example shows how to set the rate limit for incoming MLDv2-snooping packets:

```
Router(config)# ipv6 mld snooping limit rate 200
Router(config)#
```

This example shows how to configure the maximum number of entries in the explicit-tracking database:

```
Router(config)# ipv6 mld snooping limit track 20000
Router(config)#
```

This example shows how to disable software rate limiting:

```
Router(config)# no ipv6 mld snooping limit rate
Router(config)#
```

Related Commands	Command	Description
	<a href="#">ipv6 mld snooping explicit-tracking</a>	Enables explicit host tracking.
	<a href="#">show ipv6 mld snooping</a>	Displays the information about the snooping status for MLDv2 hosts.

## ipv6 mld snooping mrouter

To configure a Layer 2 port as a multicast router port, use the **ipv6 mld snooping mrouter** command.

**ipv6 mld snooping mrouter** {*interface type slot/port*}

Syntax Description	<i>interface type</i>	Specifies the interface type: valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , or <b>tengigabitethernet</b> .
	<i>slot/ports</i>	Module and port number.

**Defaults** None configured

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** To configure a static connection to a multicast router, use the [mac-address-table static](#) command.

**Examples** This example shows how to configure a Layer 2 port as a multicast router port:

```
Router(config-if)# ipv6 mld snooping mrouter interface fastethernet 5/6
Router(config-if)#
```

Related Commands	Command	Description
	<a href="#">show ipv6 mld snooping</a>	Displays MLDv2 snooping information.

# ipv6 mld snooping querier

To enable the MLDv2 snooping querier, use the **ipv6 mld snooping querier** command. To disable the MLDv2 snooping querier, use the **no** form of this command.

**ipv6 mld snooping querier**

**no ipv6 mld snooping querier**

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

**Defaults** Disabled

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Configure an IPv6 address on the VLAN interface. When enabled, the MLDv2 snooping querier uses the IPv6 address as the query source address.

If there is no IPv6 address configured on the VLAN interface, the MLDv2 snooping querier does not start. The MLDv2 snooping querier disables itself if the IPv6 address is cleared. When enabled, the MLDv2 snooping querier restarts if you configure an IPv6 address.

When enabled, the MLDv2 snooping querier does not start if it detects MLDv2 traffic from an IPv6 multicast router.

When enabled, the MLDv2 snooping querier starts after 60 seconds if it detects no MLDv2 traffic from an IPv6 multicast router.

When enabled, the MLDv2 snooping querier disables itself if it detects MLDv2 traffic from an IPv6 multicast router.

You can enable the MLDv2 snooping querier on all the Catalyst 6500 series switches in the VLAN that support it. One switch is elected as the querier.

**Examples** This example shows how to enable the MLDv2 snooping querier on VLAN 200:

```
Router# interface vlan 200
Router(config-if)# ipv6 mld snooping querier
```

Related Commands	Command	Description
	<a href="#">show ipv6 mld snooping</a>	Displays MLDv2 snooping information.

## ipv6 mld snooping report-suppression

To enable report suppression on a VLAN, use the **ipv6 mld snooping report-suppression** command. To disable report suppression on a VLAN, use the **no** form of this command.

**ipv6 mld snooping report-suppression**

**no ipv6 mld snooping report-suppression**

---

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

---

**Defaults** Enabled

---

**Command Modes** Interface configuration

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Usage Guidelines** You must enable explicit tracking before enabling report suppression. This command is supported on VLAN interfaces only.

---

**Examples** This example shows how to enable explicit host tracking:

```
Router(config-if)# ipv6 mld snooping report-suppression
Router(config-if)#
```

# ip verify unicast reverse-path

To enable unicast RPF, use the **ip verify unicast reverse-path** command. To disable unicast RPF, use the **no** form of this command.

**ip verify unicast reverse-path** [**allow-self-ping**] [*list*]

**no ip verify unicast reverse-path** [**allow-self-ping**] [*list*]

Syntax Description	<b>allow-self-ping</b>	(Optional) Allows the Catalyst 6500 series switch to ping itself.
	<i>list</i>	(Optional) Access-list number; valid values are from 1 to 199 for a standard or extended IP access-list number and from 1300 to 2699 for a standard or extended IP expanded access-list number.

**Defaults** Disabled

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Use the **ip verify unicast reverse-path** command to mitigate problems that are caused by malformed or forged (spoofed) IP source addresses that pass through a Catalyst 6500 series switch. Malformed or forged source addresses can indicate DoS attacks that are based on source IP address spoofing.



**Note**

Unicast RPF is an input function and is applied only on the input interface of a Catalyst 6500 series switch at the upstream end of a connection.

If you do not specify an ACL in the **ip verify unicast reverse-path** command, the Catalyst 6500 series switch drops the forged or malformed packet immediately and no ACL logging occurs. The Catalyst 6500 series switch and interface unicast RPF counters are updated.

You can log unicast RPF events by specifying the logging option for the ACL entries that are used by the **ip verify unicast reverse-path** command. You can use the logging option to gather information about the attack, such as the source address, time, and so on.



**Note**

With unicast RPF, all equal-cost “best” return paths are considered valid. Unicast RPF works when multiple return paths exist, if each path is equal to the others in the routing cost (such as the number of hops, weights, and so on), and the route is in the FIB. Unicast RPF also functions where EIGRP variants are used and unequal candidate paths that go back to the source IP address exist.

Do not use unicast RPF on interfaces that are internal to the network. Internal interfaces might have routing asymmetry, which means that there are multiple routes to the source of a packet. You should apply unicast RPF only where there is natural or configured symmetry.

Routers at the edge of a service-provider network are more likely to have symmetrical reverse paths than routers that are in the core of the network. Routers that are in the core of the service-provider network have no guarantee that the best forwarding path out of the router is the path that is selected for packets returning to the router.

We do not recommend that you apply unicast RPF where there is a chance of asymmetric routing. You should place unicast RPF only at the edge of a network. In a service-provider network, you should place the unicast RPF at the customer edge of the network.

---

### Examples

This example shows how to enable unicast RPF on a serial interface:

```
Router(config-if)# ip verify unicast reverse-path
Router(config-if)#
```

---

### Related Commands

Command	Description
<b>ip cef</b>	Enables CEF on the route processor.

# ip verify unicast source reachable-via

To enable and configure RPF checks, use the **ip verify unicast source reachable-via** command. To disable RPF, use the **no** form of this command.

**ip verify unicast source reachable-via** {*rx* | *any*} [**allow-default**] [**allow-self-ping**] [*list*]

**no ip verify unicast source reachable-via**

Syntax Description		
<b>rx</b>	Checks that the source address is reachable on the interface where the packet was received.	
<b>any</b>	Checks that the source address is reachable on any path.	
<b>allow-default</b>	(Optional) Checks that the default route matches the source address.	
<b>allow-self-ping</b>	(Optional) Allows the router to ping itself.	
<i>list</i>	(Optional) Access-list number; valid values are from 1 to 199 for a standard IP access-list number and from 1300 to 2699 for a standard IP expanded access-list number.	

**Defaults** Disabled

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Unicast RPF is not supported on PVLAN host ports.

Unicast RPF provides three basic modes:

- **Exists-only mode**—A source address needs to be present only in the FIB and reachable through a “real” interface; this situation also applies to the **ip verify unicast source reachable-via any allow-default** command. The exists-only mode requires that a resolved and reachable source address is present in the FIB table. The source address must be reachable through a configured interface.
- **Any mode**—The source must be reachable through any of the paths. For example, the source has per-destination load balancing.
- **Rx mode**—A source address must be reachable on the arrived interface. For example, the source must be reachable without load balancing.



**Note**

Unicast RPF is an input function and is applied only on the input interface of a router at the upstream end of a connection.

When configuring uRPF check, use the following guidelines and restrictions:

- If you configure uRPF check to filter with an ACL, the PFC determines whether or not traffic matches the ACL. The PFC sends the traffic denied by the RPF ACL to the PISA for the uRPF check. Packets permitted by the ACL are forwarded in hardware without a uRPF check. You can enter the **mls ip cef rpf hw-enable-rpf-acl** command to subject to RPF check and forwarding in hardware and the Packets that are denied by the uRPF ACL are forwarded in hardware and the packets that are permitted by ACL are sent to software.
- Because the packets in a DoS attack typically match the deny ACE and are sent to the PISA for the uRPF check, they can overload the PISA. You can enter the **mls ip cef rpf hw-enable-rpf-acl** command in these cases since DOS packets matching the deny ACE are processed in hardware.

Do not use unicast RPF on interfaces that are internal to the network. Internal interfaces might have routing asymmetry, which means that there are multiple routes to the source of a packet. You should apply unicast RPF only where there is natural or configured symmetry.

### Examples

This example shows how to enable unicast RPF exist-only checking mode:

```
Router(config-if)# ip verify unicast source reachable-via any
Router(config-if)#
```

### Related Commands

Command	Description
<b>ip cef</b>	Enables CEF on the route processor.
<a href="#">show running-config</a>	Displays the status and configuration of the module or Layer 2 VLAN.

## ip wccp group-listen

To enable the reception of IP multicast packets for WCCP, use the **ip wccp group-listen** command mode. To disable the reception of IP multicast packets for WCCP, use the **no** form of this command.

**ip wccp {web-cache | {service-number | service-name}} group-listen**

**no ip wccp {web-cache | {service-number | service-name}} group-listen**

Syntax Description	web-cache	Directs the router to send packets to the web cache service.
	<i>service-number</i>	WCCP service number; valid values are from 0 to 99.
	<i>service-name</i>	WCCP service name; the valid value is <b>web-cache</b> .

**Defaults** Disabled

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines



**Note**

To ensure that the command operates correctly, you must enter the **ip pim mode** command in addition to the **ip wccp group-listen** command.

The *service-number* may be either **web-cache** or a number representing a cache engine dynamically defined definition. Once the service is enabled, the Catalyst 6500 series switch can participate in the establishment of a service group.

On Catalyst 6500 series switches that are to be members of a service group when IP multicast is used, the following configuration is required:

- You must configure the IP multicast address for use by the WCCP service group.
- You must configure the **ip wccp {web-cache | service-number} group-listen** command on the interfaces that are to receive the IP multicast address.

### Examples

This example shows how to enable the multicast packets for a web cache with a multicast address of 224.1.1.100:

```
router# configure terminal
router(config)# ip wccp web-cache group-address 224.1.1.100
router(config)# interface ethernet 0
router(config-if)# ip wccp web-cache group-listen
```

## ■ ip wccp group-listen

Related Commands	Command	Description
	<b>ip wccp</b>	Directs a router to enable or disable the support for a cache engine service group.
	<b>ip wccp redirect</b>	Enables packet redirection on an outbound or inbound interface using WCCP.

# ip wccp redirect

To enable packet redirection on an outbound or inbound interface using WCCP, use the **ip wccp redirect** command. To disable WCCP redirection, use the **no** form of this command

```
ip wccp { web-cache | service-number } redirect { in | out }
```

```
no ip wccp { web-cache | service-number } redirect { in | out }
```

## Syntax Description

<b>web-cache</b>	Enables the web-cache service.
<i>service-number</i>	Identification number of the cache engine service group controlled by a router; valid values are from 0 to 99. If Cisco cache engines are used in the cache cluster, the <b>reverse proxy</b> service is indicated by a value of 99.
<b>redirect</b>	Enables packet redirection checking on an outbound or inbound interface.
<b>in</b>	Specifies packet redirection on an inbound interface.
<b>out</b>	Specifies packet redirection on an outbound interface.

## Defaults

Disabled

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

The **ip wccp redirect in** command allows you to configure WCCP redirection on an interface that receives inbound network traffic. When the command is applied to an interface, all packets that arrive at that interface are compared with the criteria that is defined by the specified WCCP service. If the packets match the criteria, they are redirected.

The **ip wccp redirect out** command allows you to configure the WCCP redirection check at an outbound interface.



### Note

This command can affect the **ip wccp redirect exclude in** command. If you have the **ip wccp redirect exclude in** command set on an interface and you configure the **ip wccp redirect in** command, the **ip wccp redirect exclude in** command is overridden. The opposite is also true: configuring the **ip wccp redirect exclude in** command overrides the **ip wccp redirect in** command.

For a complete description of the WCCP configuration commands, including a list of commands that have changed since Cisco IOS Release 12.0, refer to the “WCCP Commands” chapter in the “Cisco IOS System Management Commands” part of the *Cisco IOS Release 12.2 Command Reference*.

**Examples**

This example shows how to configure a session in which the reverse proxy packets on the Ethernet interface 0 are checked for redirection and are redirected to a Cisco cache engine:

```
Router# configure terminal
Router(config)# ip wccp 99
Router(config)# interface ethernet 0
Router(config-if)# ip wccp 99 redirect out
```

This example shows how to configure a session in which the HTTP traffic that arrives on interface 0/1 is redirected to a Cisco cache engine:

```
Router# configure terminal
Router(config)# ip wccp web-cache
Router(config)# interface ethernet 0/1
Router(config-if)# ip wccp web-cache redirect in
```

**Related Commands**

Command	Description
<b>show ip interface</b>	Displays the usability status of interfaces that are configured for IP.
<b>show ip wccp</b>	Displays the WCCP statistics.

# ip wccp web-cache accelerated

To enable the hardware acceleration for WCCP version 1, use the **ip wccp web-cache accelerated** command. To disable hardware acceleration, use the **no** form of this command.

```
ip wccp web-cache accelerated {[group-address groupaddress] [redirect-list access-list]
[group-list access-list] [password password]}
```

```
no ip wccp web-cache accelerated
```

## Syntax Description

<b>group-address</b> <i>groupaddress</i>	(Optional) Directs the router to use a specified multicast IP address for communication with the WCCP service group. See the “Usage Guidelines” section for additional information.
<b>redirect-list</b> <i>access-list</i>	(Optional) Directs the router to use an access list to control traffic that is redirected to this service group. See the “Usage Guidelines” section for additional information.
<b>group-list</b> <i>access-list</i>	(Optional) Directs the router to use an access list to determine which cache engines are allowed to participate in the service group. See the “Usage Guidelines” section for additional information.
<b>password</b> <i>password</i>	(Optional) Specifies a string that directs the router to apply MD5 authentication to messages received from the service group specified by the service name given. See the “Usage Guidelines” section for additional information.

## Defaults

Disabled

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

This command is supported on software releases later than cache engine software Release ACNS 4.2.1.

The **group-address** *groupaddress* option requires a multicast address that is used by the router to determine which cache engine should receive redirected messages. This option instructs the router to use the specified multicast IP address to coalesce the “I See You” responses for the “Here I Am” messages that it has received on this group address. In addition, the response is sent to the group address. The default is for no **group-address** to be configured, so that all “Here I Am” messages are responded to with a unicast reply.

The **redirect-list** *access-list* option instructs the router to use an access list to control the traffic that is redirected to the cache engines of the service group that is specified by the service-name given. The *access-list* argument specifies either a number from 1 to 99 to represent a standard or extended access-list number or a name to represent a named standard or extended access list. The access list specifies the traffic that is permitted to be redirected. The default is for no **redirect-list** to be configured (all traffic is redirected).

The **group-list** *access-list* option instructs the router to use an access list to control the cache engines that are allowed to participate in the specified service group. The *access-list* argument specifies either a number from 1 to 99 to represent a standard access-list number or a name to represent a named standard access list. The access list specifies which cache engines are permitted to participate in the service group. The default is for no **group-list** to be configured, so that all cache engines may participate in the service group.

The password can be up to seven characters. When you designate a password, the messages that are not accepted by the authentication are discarded. The password name is combined with the HMAC MD5 value to create security for the connection between the router and the cache engine.

---

### Examples

This example shows how to enable the hardware acceleration for WCCP version 1:

```
Router(config)# ip wccp web-cache accelerated
Router(config)#
```

---

### Related Commands

Command	Description
<b>ip wccp version</b>	Specifies which version of WCCP to configure on your router.

# l2protocol-tunnel

To enable the protocol tunneling on an interface and specify the type of protocol to be tunneled, use the **l2protocol-tunnel** command. To disable protocol tunneling, use the **no** form of this command.

```
l2protocol-tunnel [{cdp | stp | vtp}]
```

```
no l2protocol-tunnel [{cdp | stp | vtp}]
```

Syntax Description	cdp	(Optional) Enables CDP tunneling.
	<b>stp</b>	(Optional) Enables STP tunneling.
	<b>vtp</b>	(Optional) Enables VTP tunneling.

**Defaults** Disabled

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** On all the service provider edge switches, you must enable PortFast BPDU filtering on the 802.1Q tunnel ports by entering these commands:

```
Router(config-if)# spanning-tree bpdupfilter enable  
Router(config-if)# spanning-tree portfast
```



**Note** PortFast BPDU filtering is enabled automatically on tunnel ports.

If you do not specify a protocol, all protocols are tunneled.

You can configure protocol tunneling on VLAN and trunk interfaces.

You must enter the **switchport** command once without any keywords to configure the LAN port as a Layer 2 interface before you can enter additional **switchport** commands with keywords. This action is required only if you have not entered the **switchport** command for the interface.

**Examples** This example shows how to enable a tunneling protocol on an interface:

```
Router(config-if)# l2protocol-tunnel cdp  
Router(config-if)#
```

This example shows how to disable a tunneling protocol on an interface:

```
Router(config-if)# no l2protocol-tunnel
Protocol tunneling disabled on interface fastEthernet 4/4
Router(config-if)#
```

#### Related Commands

Command	Description
<a href="#">show</a>	Displays the protocols that are tunneled on an interface or on all interfaces.
<a href="#">l2protocol-tunnel</a>	
<a href="#">switchport</a>	Modifies the switching characteristics of the Layer 2-switched interface.

# l2protocol-tunnel cos

To specify a CoS value globally on all ingress Layer-2 protocol tunneling ports, use the **l2protocol-tunnel cos** command. To return to the default settings, use the **no** form of this command.

**l2protocol-tunnel cos** *cos-value*

**no l2protocol-tunnel cos**

Syntax Description	<i>cos-value</i>	CoS value; valid values are from 0 to 7.
--------------------	------------------	--

Defaults	The <i>cos-value</i> is 5.
----------	----------------------------

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Usage Guidelines	<p>The <i>cos-value</i> is the CoS value that you assign to the PDUs on a Layer 2-protocol tunnel port before tunneling the PDUs through the service-provider network.</p> <p>You can specify a CoS value globally on all ingress Layer 2-protocol tunneling ports. Because the CoS value applies to all ingress tunneling ports, all encapsulated PDUs that are sent out by the Catalyst 6500 series switch have the same CoS value.</p>
------------------	---

On all the service-provider edge switches, you must enable PortFast BPDU filtering on the 802.1Q tunnel ports by entering these commands:

```
Router(config-if)# spanning-tree bpdufilter enable
Router(config-if)# spanning-tree portfast
```



**Note** PortFast BPDU filtering is enabled automatically on tunnel ports.

Examples	This example shows how to specify a CoS value on all ingress Layer 2-protocol tunneling ports:
----------	--

```
Router(config)# l2protocol-tunnel cos 6
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show l2protocol-tunnel</a>	Displays the protocols that are tunneled on an interface or on all interfaces.

# l2protocol-tunnel drop-threshold

To specify the maximum number of packets that can be processed for the specified protocol on that interface before being dropped, use the **l2protocol-tunnel drop-threshold** command. To reset all the threshold values to 0 and disable the drop threshold, use the **no** form of this command.

**l2protocol-tunnel drop-threshold** [**cdp** | **stp** | **vtp**] *packets*

**no l2protocol-tunnel drop-threshold** [**cdp** | **stp** | **vtp**]

Syntax Description	
<b>cdp</b>	(Optional) Specifies CDP packets.
<b>stp</b>	(Optional) Specifies STP packets.
<b>vtp</b>	(Optional) Specifies VTP packets.
<i>packets</i>	Maximum number of packets; valid values are from 1 to 4096 packets.

**Defaults** Disabled

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** On all the service-provider edge switches, you must enable PortFast BPDU filtering on the 802.1Q tunnel ports by entering these commands:

```
Router(config-if)# spanning-tree bpdupfilter enable
Router(config-if)# spanning-tree portfast
```



**Note** PortFast BPDU filtering is enabled automatically on tunnel ports.

If you do not specify a protocol, the threshold applies to all protocols.

You can configure protocol tunneling on switch ports only. You must enter the **switchport** command once without any keywords to configure the LAN port as a Layer 2 interface before you can enter additional **switchport** commands with keywords. This action is required only if you have not entered the **switchport** command for the interface.

Refer to the “Configuring IEEE 802.1Q Tunneling and Layer 2 Protocol Tunneling” chapter of the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY* for additional information on setting the drop threshold value.

**Examples**

This example shows how to set the drop threshold:

```
Router(config-if)# switchport
Router(config-if)# l2protocol-tunnel drop-threshold 3000
Router(config-if)#
```

**Related Commands**

Command	Description
<b>l2protocol-tunnel</b>	Enables the protocol tunneling on an interface and specifies the type of protocol to be tunneled.
<b>l2protocol-tunnel cos</b>	Specifies a CoS value globally on all ingress Layer-2 protocol tunneling ports.
<b>l2protocol-tunnel global drop-threshold</b>	Enables rate limiting at the software level.
<b>l2protocol-tunnel shutdown-threshold</b>	Specifies the maximum number of packets that can be processed for the specified protocol on that interface in 1 second.
<b>show l2protocol-tunnel</b>	Displays the protocols that are tunneled on an interface or on all interfaces.
<b>switchport</b>	Modifies the switching characteristics of the Layer 2-switched interface.

## l2protocol-tunnel global drop-threshold

To enable rate limiting at the software level, use the **l2protocol-tunnel global drop-threshold** command. To disable the software rate limiter on the Catalyst 6500 series switch, use the **no** form of this command.

**l2protocol-tunnel global drop-threshold** *threshold*

**no l2protocol-tunnel global drop-threshold**

<b>Syntax Description</b>	<i>threshold</i>	Maximum rate of incoming PDUs before excessive PDUs are dropped; valid values are from 100 to 20000 PDUs.
---------------------------	------------------	---

<b>Defaults</b>	Global thresholds are not configured.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	All three PDUs (normal BPDU, CDP, and VTP packets) that arrive on Layer 2-protocol tunnel-enabled ports are rate limited. Rate limiting occurs in the ingress direction in Layer 2-protocol tunneling. If the rate of the incoming PDUs exceeds the configured <i>threshold</i> , the excessive PDUs are dropped.
-------------------------	---

<b>Examples</b>	This example shows how to enable rate limiting globally:
-----------------	--

```
Router(config)# l2protocol-tunnel global drop-threshold 3000
Router(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">l2protocol-tunnel</a>	Enables the protocol tunneling on an interface and specifies the type of protocol to be tunneled.
	<a href="#">l2protocol-tunnel cos</a>	Specifies a CoS value globally on all ingress Layer-2 protocol tunneling ports.
	<a href="#">l2protocol-tunnel drop-threshold</a>	Specifies the maximum number of packets that can be processed for the specified protocol on that interface before being dropped.
	<a href="#">l2protocol-tunnel shutdown-threshold</a>	Specifies the maximum number of packets that can be processed for the specified protocol on that interface in 1 second.
	<a href="#">show l2protocol-tunnel</a>	Displays the protocols that are tunneled on an interface or on all interfaces.

# l2protocol-tunnel shutdown-threshold

To specify the maximum number of packets that can be processed for the specified protocol on that interface in 1 second, use the **l2protocol-tunnel shutdown-threshold** command. To reset all the threshold values to 0 and disable the shutdown threshold, use the **no** form of this command.

```
l2protocol-tunnel shutdown-threshold [cdp | stp | vtp] packets
```

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

## Syntax Description

<b>cdp</b>	(Optional) Specifies CDP tunneling.
<b>stp</b>	(Optional) Specifies STP tunneling.
<b>vtp</b>	(Optional) Specifies VTP tunneling.
<i>packets</i>	Shutdown threshold; valid values are from 1 to 4096.

## Defaults

This command has no default settings.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

When the number of *packets* is exceeded, the port is put in error-disabled state.

On all the service-provider edge switches, you must enable PortFast BPDU filtering on the 802.1Q tunnel ports by entering these commands:

```
Router(config-if)# spanning-tree bpdupfilter enable  
Router(config-if)# spanning-tree portfast
```



### Note

PortFast BPDU filtering is enabled automatically on tunnel ports.

If you do not specify a protocol, the *packets* value applies to all protocols.

You can configure protocol tunneling on switch ports only. You must enter the **switchport** command once without any keywords to configure the LAN port as a Layer 2 interface before you can enter additional **switchport** commands with keywords. This action is required only if you have not entered the **switchport** command for the interface.

Refer to the “Configuring IEEE 802.1Q Tunneling and Layer 2 Protocol Tunneling” chapter of the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY* for additional information on setting the drop threshold value.

**Examples**

This example shows how to specify the maximum number of CDP packets that can be processed on that interface in 1 second:

```
Router(config-if)# switchport
Router(config-if)# l2protocol-tunnel shutdown-threshold cdp 200
Router(config-if)#
```

**Related Commands**

Command	Description
<b>l2protocol-tunnel</b>	Enables the protocol tunneling on an interface and specifies the type of protocol to be tunneled.
<b>show l2protocol-tunnel</b>	Displays the protocols that are tunneled on an interface or on all interfaces.
<b>switchport</b>	Modifies the switching characteristics of the Layer 2-switched interface.

## l2 vfi manual

To create a Layer 2 VFI and enter the Layer 2 VFI manual configuration submode, use the **l2 vfi manual** command. To remove the Layer 2 VFI, use the **no** form of this command.

**l2 vfi** *name* **manual**

**no l2 vfi** *name* **manual**

Syntax Description	<i>name</i>	Name of a new or existing Layer 2 VFI.
--------------------	-------------	--

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

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Usage Guidelines	A VFI is a collection of data structures used by the data plane, software-based or hardware-based, to forward packets to one or more VCs. It is populated and updated by both the control plane and the data plane and also serves as the data structure interface between the control plane and the data plane.
------------------	--

Within the Layer 2 VFI manual configuration submode, you can configure the following parameters:

- VPN ID of a VPLS domain
- Addresses of other PE routers in this domain
- Type of tunnel signaling and encapsulation mechanism for each peer

Within the Layer 2 VFI manual configuration submode, the following commands are available:

- **[no] vpn id** *vpn-id*—Configures a VPN ID in RFC 2685 format. To remove the VPN ID from the configuration, use the **no** form of this command.
- **[no] neighbor** *remote-router-id* { **encapsulation** { **l2tpv3** | **mpls** } | { **pw-class** *pw-name* } | **no-split-horizon** }—Specifies the type of tunnel signaling and encapsulation mechanism for each peer. See the **neighbor** command.

Examples	This example shows how to create a Layer 2 VFI, enter the Layer 2 VFI manual configuration submode, and configure a VPN ID:
----------	---

```
Router(config)# l2 vfi vfitest1 manual
Router(config-vfi)# vpn id 303
```

# lacp max-bundle

To define the maximum number of bundled LACP ports allowed in this port channel, use the **lacp max-bundle** command. To return to the default settings, use the **no** form of this command.

**lacp max-bundle** *max-bundles*

**no lacp max-bundle**

Syntax Description	<i>max-bundles</i>	Maximum number of bundled ports allowed in this port channel; valid values are from 1 to 8.
--------------------	--------------------	---

Defaults	The default settings are as follows: <ul style="list-style-type: none"> <li>• Maximum of eight bundled ports.</li> <li>• Maximum of eight bundled ports and eight hot-standby ports per port channel; this setting applies if the port channel on both sides of the LACP bundle are configured the same.</li> </ul>
----------	---

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to set the maximum number of ports to bundle in this port channel:

```
Router(config-if)# lacp max-bundle 4
Router(config-if)#
```

Related Commands	Command	Description
	<a href="#">show lacp</a>	Displays LACP information.

# lACP port-priority

To set the priority for the physical interfaces, use the **lACP port-priority** command.

**lACP port-priority** *priority*

<b>Syntax Description</b>	<i>priority</i>	Priority for the physical interfaces; valid values are from 1 to 65535.
---------------------------	-----------------	---

<b>Defaults</b>	<b>32768</b>
-----------------	--------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

You must assign a port priority to each port in the Catalyst 6500 series switch. You can specify the port priority 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, *priority* is supported only on port channels with LACP-enabled physical interfaces.

This command is supported on LACP-enabled interfaces.

When setting the priority, note that a higher number means a lower priority.

**Examples**

This example shows how to set the priority for the interface:

```
Router(config-if)# lACP port-priority 23748
Router(config-if)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">channel-group</a>	Assigns and configures an EtherChannel interface to an EtherChannel group.
	<a href="#">channel-protocol</a>	Sets the protocol that is used on an interface to manage channeling.
	<a href="#">lACP system-priority</a>	Sets the priority of the system.
	<a href="#">show lACP</a>	Displays LACP information.

# lacp rate

To set the rate at which the LACP packets are ingressed to an interface, use the **lacp rate** command. To return to the default settings, use the **no** form of this command.

**lacp rate {normal | fast}**

**no lacp rate**

Syntax Description	normal	fast
	Specifies that the LACP packets are ingressed at the normal rate of 30-seconds rate.	Specifies that the LACP packets are ingressed at the fast rate of 1-second rate once the link is established.

**Defaults** 90 seconds

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command is supported on LACP-enabled interfaces.

**Examples** This example shows how to specify that the LACP packets are ingressed at the one-second rate:

```
Router(config-if)# lacp rate fast
Router(config-if)#
```

Related Commands	Command	Description
	<a href="#">show lacp</a>	Displays LACP information.

# lACP system-priority

To set the priority of the system, use the **lACP system-priority** command.

**lACP system-priority** *priority*

<b>Syntax Description</b>	<i>priority</i>	Priority of the system; valid values are from 1 to 65535.
---------------------------	-----------------	---

<b>Defaults</b>	<b>32768</b>
-----------------	--------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** You must assign a system priority to each Catalyst 6500 series switch running LACP. You can specify the system priority automatically or by entering the **lACP system-priority** command. The system priority is used with the Catalyst 6500 series switch MAC address to form the system ID and is also used during negotiation with other systems.

Although this command is a global configuration command, *priority* is supported on port channels with LACP-enabled physical interfaces.

When setting the priority, note that a higher number means a lower priority.

You can also enter the **lACP system-priority** command. Once you enter the command, the system defaults to global configuration mode.

**Examples** This example shows how to set the system priority:

```
Router(config)# lACP system-priority 23748
Router(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">channel-group</a>	Assigns and configures an EtherChannel interface to an EtherChannel group.
	<a href="#">channel-protocol</a>	Sets the protocol that is used on an interface to manage channeling.
	<a href="#">lACP port-priority</a>	Sets the priority for the physical interfaces.
	<a href="#">show lACP</a>	Displays LACP information.

# line

To identify a specific line for configuration and enter line configuration collection mode, use the **line** command.

```
line {{ first-line-number [ending-line-number] } | { console first-line-number } | { vtty
first-line-number [ending-line-number] } }
```

Syntax Description		
<i>first-line-number</i>		Relative number of the terminal line (or the first line in a contiguous group) that you want to configure when the line type is specified; valid values are from 0 to 1510.
<i>ending-line-number</i>		(Optional) Relative number of the last line in a contiguous group that you want to configure; valid values are from 101 to 1510.
<b>console</b> <i>first-line-number</i>		Specifies the console terminal line; the valid value is <b>0</b> .
<b>vtty</b>		Specifies the virtual terminal line for remote console access.

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

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The console port is DCE.

If you do not specify **console** or **vtty**, the *first-line-number* and *ending-line-number* are absolute rather than relative line numbers.

You can address a single line or a consecutive range of lines with the **line** command. A line number is necessary, though, and you will receive an error message if you forget to include it.

Entering the **line** command with the optional line type (**console** or **vtty**) designates the line number as a relative line number. For example, to configure line parameters for line 7 (a TTY line), you could enter the **line tty 7** command.

You also can use the **line** command without specifying a line type. In this case, the line number is treated as an absolute line number. For example, to configure line parameters for line 5, which can be of any type, you could enter the **line 5** command.

Absolute line numbers increment consecutively and can be difficult to manage on large systems. Relative line numbers are a shorthand notation used in configurations. Internally, the Cisco IOS software uses absolute line numbers. You cannot use relative line numbers everywhere, but you can use absolute line numbers everywhere.

You can enter the **show users all** command to display a table of absolute and relative line numbers. The absolute line numbers are listed at the far left, followed by the line type, and then the relative line number. Relative line numbers always begin at zero and define the type of line. Addressing the second virtual terminal line as line VTY 1, for example, is easier than remembering it as line 143—its absolute line number.

The terminal from which you locally configure the router is attached to the console port. To configure line parameters for the console port, enter the **line console 0** command. The console relative line number must be **0**.

Once you enter the line console configuration mode, you can set the transmit and receive speeds; valid values are from 0 to 9600. The default rate is 9600.

Virtual terminal lines are used to allow remote access to the router. A virtual terminal line is not associated with either the auxiliary or console port. The router has five virtual terminal lines by default. However, you can create additional virtual terminal lines as described in the chapter “Configuring Protocol Translation and Virtual Asynchronous Devices” in the *Cisco IOS Terminal Services Configuration Guide*.

Configuring the console port or virtual terminal lines allows you to perform such tasks as setting communication parameters, specifying autobaud connections, and configuring terminal operating parameters for the terminal that you are using.

## Examples

This example shows how to start the configuration for virtual terminal lines 0 to 4:

```
Router(config)# line vty 0 4
Router(config-line)#
```

This example shows how to create and configure the maximum 100 virtual terminal lines with the **no login** command:

```
Router(config)# line vty 0 99
Router(config-line)# no login
Router(config-line)#
```

This example shows how to eliminate the virtual terminal line number 5 and all higher-numbered virtual terminal lines. Only virtual terminal lines 0 to 4 will remain.

```
Router(config-line)# no line vty 5
Router(config)#
```

This example shows how to set the transmit and receive speeds for the console port:

```
Router(config)# line console 0
Router(config-line)# speed 9600
Router(config-line)#
```

## Related Commands

Command	Description
<b>show line</b>	Displays parameters of a terminal line.
<b>show users</b>	Displays information about the active lines on the router.

# link debounce

To enable the debounce timer on an interface, use the **link debounce** command. To disable the timer, use the **no** form of this command.

**link debounce** [*time time*]

**no link debounce**

Syntax Description	<b>time time</b>
	(Optional) Specifies the extended debounce timer; valid values are from 100 to 5000 milliseconds.

## Defaults

Table 2-13 lists the debounce timer defaults.

*Table 2-13 Port Debounce Timer Delay Time*

Port Type	Debounce Timer Disabled	Debounce Timer Enabled
10BASE-FL ports	300 milliseconds	3100 milliseconds
10/100BASE-TX ports	300 milliseconds	3100 milliseconds
100BASE-FX ports	300 milliseconds	3100 milliseconds
10/100/1000BASE-TX ports	300 milliseconds	3100 milliseconds
1000BASE-TX ports	300 milliseconds	3100 milliseconds
Fiber Gigabit ports	10 milliseconds	100 milliseconds
10-Gigabit ports except WS-X6501-10GEX4 and WS-X6502-10GE	10 milliseconds	100 milliseconds
WS-X6501-10GEX4 and WS-X6502-10GE 10-Gigabit ports	1000 milliseconds	3100 milliseconds

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

The **time time** keyword and argument are supported on Gigabit Ethernet and 10-Gigabit Ethernet interfaces only.

The **time time** keyword and argument are not supported on copper media.

The debounce timer sets the amount of time that the firmware waits before it notifies the software that the link is down. The debounce timer does not apply to linkup because the linkup is immediately notified by the firmware.

The default debounce time applies when you enter the **link debounce** command with no arguments. For example, when you enter the **link debounce time 100** command, it is equivalent to entering the **link debounce** command with no arguments. You will see the following link debounce entry in the configuration:

```
interface GigabitEthernet4/4
  no ip address
  link debounce
```

Enter the **show interfaces debounce** command to display the debounce configuration of an interface.

---

### Examples

This example shows how to configure the debounce timer on a Gigabit Ethernet fiber interface:

```
Router (config-if)# link debounce time 100
Router (config-if)#
```

---

### Related Commands

Command	Description
<b>show interfaces debounce</b>	Displays the status and configuration for the debounce timer.

---

# load-interval

To specify the length of time to be used to calculate the average load for an interface, use the **load-interval** command. To return to the default settings, use the **no** form of this command.

**load-interval** *seconds*

**no load-interval**

<b>Syntax Description</b>	<i>seconds</i>	Length of time that is used to compute load statistics; valid values are from 30 to 600 seconds in 30-second increments.
---------------------------	----------------	--

<b>Defaults</b>	300 seconds (5 minutes)
-----------------	-------------------------

<b>Command Modes</b>	Interface configuration Frame Relay DLCI configuration
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

By default, the load data is gathered every 5 minutes or 300 seconds. You can use this data to compute load statistics, including the input rate in bits and packets per second, and the output rate in bits and packets per second, load, and reliability. Load data is computed using a weighted-average calculation where recent load data has more weight than older load data.

If you want the load computations to be more reactive to short bursts of traffic, rather than being averaged over 5-minute periods, you can shorten the length of time over which load averages are computed. For example, you can set the load interval to 30 seconds to reflect the weighted-average load for the last 30-second period.

Enter the **load-interval** command to change the calculation interval from the default value of 5 minutes (300 seconds) to a shorter or longer period of time. If you change it to a shorter period of time, the input and output statistics that are displayed when you use the **show interface** or **show frame-relay pvc** command will be more current, rather than reflecting a more average load over a longer period of time.

Enter the **load-interval** command to increase or decrease the likelihood of activating a backup interface; for example, a backup dial interface may be triggered by a sudden spike in the load on an active interface.

---

**Examples**

This example shows how to set the load interval for the serial interface 0 so that the average is computed over 30-second intervals:

```
Router(config)# interface serial 0
Router(config-if)# load-interval 30
```

This example shows how to set the load interval to 60 seconds for a Frame Relay PVC with the DLCI 100:

```
Router(config)# interface serial 1/1
Router(config-if)# encapsulation frame-relay ietf
Router(config-if)# frame-relay interface-dlci 100
Router(config-fr-dlci)# load-interval 60
```

---

**Related Commands**

Command	Description
<b>show frame-relay pvc</b>	Displays statistics about PVCs for Frame Relay interfaces.

---

# logging event link-status (global configuration)

To change the default or set the link-status event messaging during system initialization, use the **logging event link-status** command. To disable the link-status event messaging, use the **no** form of this command.

**logging event link-status { default | boot }**

**no logging event link-status { default | boot }**

Syntax Description	default	Enables system logging of interface state-change events on all interfaces in the system.
	<b>boot</b>	Enables system logging of interface state-change events on all interfaces in the system during system initialization.

**Defaults** Interface state-change messages are not sent.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** You do not have to enter the **logging event link-status boot** command to enable link-status messaging during system initialization. The **logging event link-status default** command logs system messages even during system initialization.

If you enter both the **logging event link-status default** and the **no logging event link-status boot** commands, the interface state-change events are logged after all modules in the Catalyst 6500 series switch come online after system initialization. The **logging event link-status default** and the **no logging event link-status boot** commands are saved and retained in the running configuration of the system.

When both the **logging event link-status default** and the **no logging event link-status boot** commands are present in the running configuration and you want to display the interface state-change messages during system initialization, enter the **logging event link-status boot** command.

**Examples** This example shows how to enable the system logging of the interface state-change events on all interfaces in the system:

```
Router(config)# logging event link-status default
Router(config)#
```

This example shows how to enable the system logging of interface state-change events on all interfaces during system initialization:

```
Router(config)# logging event link-status boot
Router(config)#
```

This example shows how to disable the system logging of interface state-change events on all interfaces:

```
Router(config)# no logging event link-status default
Router(config)#
```

This example shows how to disable the system logging of interface state-change events during system initialization:

```
Router(config)# no logging event link-status boot
Router(config)#
```

---

**Related Commands**

Command	Description
<a href="#">show running-config</a>	Displays the status and configuration of the module or Layer 2 VLAN.

---

# logging event link-status (interface configuration)

To enable the link-status event messaging on an interface, use the **logging event link-status** command. To disable the link-status event messaging, use the **no** form of this command.

**logging event link-status**

**no logging event link-status**

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

**Defaults** Interface state-change messages are not sent.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** To enable system logging of interface state-change events on a specific interface, enter the **logging event link-status** command.

To enable system logging of interface state-change events on all interfaces in the system, enter the **logging event link-status** command.

**Examples** This example shows how to enable the system logging of the interface state-change events on an interface:

```
Router(config-if)# logging event link-status
Router(config-if)#
```

This example shows how to disable the system logging of the interface state-change events on an interface:

```
Router(config-if)# no logging event link-status default
Router(config-if)#
```

Related Commands	Command	Description
	<a href="#">show running-config</a>	Displays the status and configuration of the module or Layer 2 VLAN.

# logging event subif-link-status

To enable the link-status event messaging on a subinterface, use the **logging event subif-link-status** command. To disable the link-status event messaging on a subinterface, use the **no** form of this command.

**logging event subif-link-status**

**no logging event subif-link-status**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Subinterface state-change messages are not sent.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

This command is supported on the following subinterfaces:

- Frame Relay subinterfaces
- OSM-GE-WAN subinterfaces
- SIP subinterfaces
- LAN subinterfaces

To enable system logging of interface state-change events on a specific subinterface, enter the **logging event subif-link-status** command.

To enable system logging of interface state-change events on a specific interface, enter the **logging event link-status** command.

To enable system logging of interface state-change events on all interfaces in the system, enter the **logging event link-status** command.

## Examples

This example shows how to enable the system logging of the interface state-change events on a subinterface:

```
Router(config-if)# logging event subif-link-status
Router(config-if)#
```

## ■ logging event subif-link-status

This example shows how to disable the system logging of the interface state-change events on a subinterface:

```
Router(config-if)# no logging event subif-link-status
Router(config-if)#
```

---

**Related Commands**

Command	Description
<a href="#">show running-config</a>	Displays the status and configuration of the module or Layer 2 VLAN.

---

# logging ip access-list cache (global configuration mode)

To configure the OAL parameters, use the **logging ip access-list cache** command. To return to the default settings, use the **no** form of this command.

```
logging ip access-list cache {{entries entries} | {interval seconds} | {rate-limit pps} |
{threshold packets}}
```

```
no logging ip access-list cache [entries | interval | rate-limit | threshold]
```

## Syntax Description

<b>entries</b> <i>entries</i>	Specifies the maximum number of log entries that are cached in the software; valid values are from 0 to 1048576 entries.
<b>interval</b> <i>seconds</i>	Specifies the maximum time interval before an entry is sent to syslog; valid values are from 5 to 86400 seconds.
<b>rate-limit</b> <i>pps</i>	Specifies the number of packets that are logged per second in the software; valid values are from 10 to 1000000 pps.
<b>threshold</b> <i>packets</i>	Specifies the number of packet matches before an entry is sent to syslog; valid values are from 1 to 1000000 packets.

## Defaults

The defaults are as follows:

- **entries**—**8000** entries.
- **seconds**—**300** seconds (5 minutes).
- **rate-limit pps**—**0** (rate limiting is off) and all packets are logged.
- **threshold packets**—**0** (rate limiting is off) and the system log is not triggered by the number of packet matches.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

OAL is supported on IPv4 unicast traffic only.

You cannot configure OAL and VACL capture on the same chassis. OAL and VACL capture are incompatible. With OAL configured, use SPAN to capture traffic.

If the entry is inactive for the duration that is specified in the **update-interval seconds** command, the entry is removed from the cache.

If you enter the **no logging ip access-list cache** command without keywords, all the parameters are returned to the default values.

You must set ICMP unreachable rate limiting to 0 if the OAL is configured to log denied packets.

**Examples**

This example shows how to specify the maximum number of log entries that are cached in the software:

```
Router(config)# logging ip access-list cache entries 200
Router(config)#
```

This example shows how to specify the maximum time interval before an entry is sent to the system log:

```
Router(config)# logging ip access-list cache interval 350
Router(config)#
```

This example shows how to specify the number of packets that are logged per second in the software:

```
Router(config)# logging ip access-list cache rate-limit 100
Router(config)#
```

This example shows how to specify the number of packet matches before an entry is sent to the system log:

```
Router(config)# logging ip access-list cache threshold 125
Router(config)#
```

**Related Commands**

Command	Description
<a href="#">clear logging ip access-list cache</a>	Clears all the entries from the OAL cache and sends them to the syslog.
<a href="#">logging ip access-list cache (interface configuration mode)</a>	Enables an OAL-logging cache on an interface that is based on direction.
<a href="#">show logging ip access-list</a>	Displays information about the logging IP access list.

# logging ip access-list cache (interface configuration mode)

To enable an OAL-logging cache on an interface that is based on direction, use the **logging ip access-list cache** command. To disable OAL, use the **no** form of this command.

**logging ip access-list cache** [**in** | **out**]

**no logging ip access-list cache**

## Syntax Description

<b>in</b>	(Optional) Enables OAL on ingress packets.
<b>out</b>	(Optional) Enables OAL on egress packets.

## Defaults

Disabled

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

This command is supported on traffic that matches the **log** keyword in the applied ACL. You must set ICMP unreachable rate limiting to 0 if the OAL is configured to log denied packets.

On systems that are configured with a PFC3A, support for the egress direction on tunnel interfaces is not supported.

OAL is supported on IPv4 unicast traffic only.

You cannot configure OAL and VACL capture on the same chassis. OAL and VACL capture are incompatible. With OAL configured, use SPAN to capture traffic.

If the entry is inactive for the duration that is specified in the **update-interval** *seconds* command, the entry is removed from the cache.

If you enter the **no logging ip access-list cache** command without keywords, all the parameters are returned to the default values.

## Examples

This example shows how to enable OAL on ingress packets:

```
Router(config-if)# logging ip access-list cache in
Router(config-if)#
```

## ■ logging ip access-list cache (interface configuration mode)

This example shows how to enable OAL on egress packets:

```
Router(config-if)# logging ip access-list cache out
Router(config-if)#
```

Related Commands	Command	Description
	<a href="#">clear logging ip access-list cache</a>	Clears all the entries from the OAL cache and sends them to the syslog.
	<a href="#">logging ip access-list cache (global configuration mode)</a>	Configures the OAL parameters.
	<a href="#">show logging ip access-list</a>	Displays information about the logging IP access list.

# mac access-list extended

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

**mac access-list extended** *name*

**no mac access-list extended** *name*

<b>Syntax Description</b>	<i>name</i> Name of the ACL to which the entry belongs.				
<b>Defaults</b>	No default ACL				
<b>Command Modes</b>	Global configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(18)ZY</td> <td>Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)ZY	Support for this command was introduced.
Release	Modification				
12.2(18)ZY	Support for this command was introduced.				

## Usage Guidelines

When you enter the ACL name, follow these naming conventions:

- Maximum of 31 characters and may 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**

You can configure named ACLs that filter IPX, DECnet, AppleTalk, VINES, or XNS traffic based on MAC addresses (IPX filtering with a MAC ACL is supported only with a PFC3).

In systems that are configured with PFC3, if you want to classify all IPX traffic by using a MAC-access list that matches on EtherType 0x8137, use the **ipx-arpa** or **ipx-non-arpa** protocol.

Once you enter the **mac access-list extended** *name* command, use the following subset to create or delete entries in a MAC-access list:

```
[no] {permit | deny} {{src-mac mask | any} {dest-mac mask} | any} [protocol [vlan vlan]
[cos value]]
```

The **vlan** *vlan* and **cos** *value* keywords and arguments are supported in PFC3BXL or PFC3B mode.

The **vlan** *vlan* and **cos** *value* keywords and arguments are not supported on the MAC VACLs.

Table 2-14 describes the syntax of the **mac access-list extended** subcommands.

**Table 2-14** *mac access-list extended Subcommands*

Subcommand	Description
<b>no</b>	(Optional) Deletes a statement from an access list.
<b>permit</b>	Permits access if the conditions are matched.
<b>deny</b>	Denies access if the conditions are matched.
<i>src-mac mask</i>	Source MAC address in the form: <i>source-mac-address source-mac-address-mask</i> .
<b>any</b>	Specifies any protocol type.
<i>dest-mac mask</i>	(Optional) Destination MAC address in the form: <i>dest-mac-address dest-mac-address-mask</i> .
<i>protocol</i>	(Optional) Name or number of the protocol; see below for a list of valid values.
<b>vlan vlan</b>	(Optional) Specifies a VLAN ID; valid values are from 0 to 4095.
<b>cos value</b>	(Optional) Specifies a CoS value; valid values are from 0 to 7.

Valid protocol names are as follows:

- 0x0-0xFFFF—Arbitrary EtherType in hex
- **aarp**—EtherType: AppleTalk ARP
- **amber**—EtherType: DEC-Amber
- **appletalk**—EtherType: AppleTalk/EtherTalk
- **dec-spanning**—EtherType: DEC-Spanning-Tree
- **decnet-iv**—EtherType: DECnet Phase IV
- **diagnostic**—EtherType: DEC-Diagnostic
- **dsm**—EtherType: DEC-DSM
- **etype-6000**—EtherType: 0x6000
- **etype-8042**—EtherType: 0x8042
- **ip**—EtherType: 0x0800
- **ipx-arpa**—IPX arpa
- **ipx-non-arpa**—IPX non arpa
- **lat**—EtherType: DEC-LAT
- **lavc-sca**—EtherType: DEC-LAVC-SCA
- **mop-console**—EtherType: DEC-MOP Remote Console
- **mop-dump**—EtherType: DEC-MOP Dump
- **msdos**—EtherType: DEC-MSDOS
- **mumps**—EtherType: DEC-MUMPS
- **netbios**—EtherType: DEC-NETBIOS
- **vines-echo**—EtherType: VINES Echo

- **vines-ip**—EtherType: VINES IP
- **xns-idp**—EtherType: XNS IDP

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

- Enter MAC addresses as three 4-byte values in dotted hexadecimal format (for example, 0030.9629.9f84).
- Enter MAC-address masks as three 4-byte values in dotted hexadecimal format. Use 1 bit as a wildcard. For example, to match an address exactly, use 0000.0000.0000 (can be entered as 0.0.0).
- For the optional *protocol*, you can enter either the EtherType or the keyword.
- Entries without a *protocol* match any protocol.
- Access lists 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.

Malformed, invalid, deliberately corrupt EtherType 0x800 IP frames are not recognized as IP traffic and are not filtered by IP ACLs.

An ACE created with the **mac access-list extended** command with the **ip** keyword filters malformed, invalid, deliberately corrupt EtherType 0x800 IP frames only; it does not filter any other IP traffic.

### Examples

This example shows how to create a MAC-access list named `mac_layer` that denies traffic from 0000.4700.0001, which is going to 0000.4700.0009, and permits all other traffic:

```
Router(config)# mac access-list extended mac_layer
Router(config-ext-macl)# deny 0000.4700.0001 0.0.0 0000.4700.0009 0.0.0 dsm
Router(config-ext-macl)# permit any any
```

### Related Commands

Command	Description
<a href="#">show mac-address-table</a>	Displays information about the MAC-address table.

## mac-address-table aging-time

To configure the aging time for entries in the Layer 2 table, use the **mac-address-table aging-time** command. To return to the default settings, use the **no** form of this command.

**mac-address-table aging-time** *seconds* [**routed-mac** | **vlan** *vlan-id*]

**no mac-address-table aging-time** *seconds* [**routed-mac** | **vlan** *vlan-id*]

<b>Syntax Description</b>	<i>seconds</i>	Aging time; valid values are 0 and from 5 to 1000000 seconds.
	<b>routed-mac</b>	(Optional) Specifies the routed MAC aging interval.
	<b>vlan</b> <i>vlan-id</i>	(Optional) Specifies the VLAN to apply the changed aging time; valid values are from 1 to 4094.

**Defaults** 300 seconds

**Command Modes** Global configuration

<b>Command History</b>	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

If you do not enter a VLAN, the change is applied to all routed-port VLANs.

Enter **0** seconds to disable aging.

You can enter the **routed-mac** keyword to configure the MAC address aging time for traffic that has the routed MAC (RM) bit set.

---

**Examples**

This example shows how to configure the aging time:

```
Router(config)# mac-address-table aging-time 400
Router(config)#
```

This example shows how to change the RM aging time:

```
Router(config)# mac-address-table aging-time 500 routed-mac
Router(config)#
```

This example shows how to disable aging:

```
Router(config)# mac-address-table aging-time 0
Router(config)
```

---

**Related Commands**

Command	Description
<a href="#">show mac-address-table</a>	Displays information about the MAC-address table.

# mac-address-table learning

To enable MAC-address learning, use the **mac-address-table learning** command. To disable learning, use the **no** form of this command.

```
[default] mac-address-table learning {{vlan vlan-id} | {vlans vlan-range} | {interface interface slot/port}} [module num]
```

```
no mac-address-table learning {{vlan vlan-id} | {vlans vlan-range} | {interface interface slot/port}} [module num]
```

Syntax Description	default	(Optional) Returns to the default settings.
	<b>vlan</b> <i>vlan-id</i>	Specifies the VLAN to apply the per-VLAN learning of all MAC addresses; valid values are from 1 to 4094.
	<b>vlans</b> <i>vlan-range</i>	Specifies the number of the VLANs to be mapped to the specified instance; valid values are from 1 to 4094.
	<b>interface</b> <i>interface slot/port</i>	Specifies per-interface based learning of all MAC addresses.
	<i>interface slot/port</i>	Interface type, the slot number, and the port number.
	<b>module</b> <i>num</i>	(Optional) Specifies the module number.

**Defaults** If you configure a VLAN on a port in a module, all the supervisor engines and DFCs in the Catalyst 6500 series switch are enabled to learn all the MAC addresses on the specified VLAN.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.
	12.(23)SXH	This command was changed to allow you to enter a range of VLANs.

**Usage Guidelines** You can use the **module** *num* keyword and argument to specify supervisor engines or DFCs only.

You can use the **vlan** *vlan-id* keyword and argument on switch-port VLANs only. You cannot use the **vlan** *vlan-id* keyword and argument to configure learning on routed interfaces.

You can use the **interface** *interface slot/port* keyword and arguments on routed interfaces and supervisor engines only. You cannot use the **interface** *interface slot/port* keyword and arguments to configure learning on switch-port interfaces.

In releases after Cisco IOS Release 12.(23)SXH, you can enter a range of VLANS separated by a hyphen.

**Examples**

This example shows how to enable MAC-address learning on a switch-port interface on all modules:

```
Router (config)# mac-address-table learning vlan 100
Router (config)#
```

This example shows how to enable MAC-address learning on a range of VLANs on all modules:

```
Router (config)# mac-address-table learning vlan 100-115,125
Router (config)#
```

This example shows how to enable MAC-address learning on a switch-port interface on a specified module:

```
Router (config)# mac-address-table learning vlan 100 module 4
Router (config)#
```

This example shows how to disable MAC-address learning on a specified switch-port interface for all modules:

```
Router (config)# no mac-address-table learning vlan 100
Router (config)#
```

This example shows how to enable MAC-address learning on a routed interface on all modules:

```
Router (config)# mac-address-table learning vlan 100
Router (config)#
```

This example shows how to enable MAC-address learning on a routed interface for a specific module:

```
Router (config)# mac-address-table learning interface FastEthernet 3/48 module 4
Router (config)#
```

This example shows how to disable MAC-address learning for all modules on a specific routed interface:

```
Router (config)# no mac-address-table learning interface FastEthernet 3/48
Router (config)#
```

**Related Commands**

Command	Description
<a href="#">show mac-address-table learning</a>	Displays the MAC-address learning state.

## mac-address-table limit

To enable MAC limiting, use the **mac-address-table limit** command. To disable MAC limiting, use the **no** form of this command.

```
mac-address-table limit [maximum num] [action { warning | limit | shutdown}]
[notification { syslog | trap | both}]
```

```
mac-address-table limit [{vlan vlan} | {interface type mod/port}] [maximum num] [action
{warning | limit | shutdown}] [flood]
```

```
no mac-address-table limit [vlan vlan] [maximum | action]
```

Syntax Description	
<b>maximum num</b>	(Optional) Specifies the maximum number of MAC entries per VLAN per EARL allowed; valid values are from 5 to 32000 MAC-address entries.
<b>action</b>	(Optional) Specifies the type of action to be taken when the action is violated.
<b>warning</b>	Specifies that the one syslog message will be sent and no further action will be taken when the action is violated.
<b>limit</b>	Specifies that the one syslog message will be sent and/or a corresponding trap will be generated with the MAC limit when the action is violated.
<b>shutdown</b>	Specifies that the one syslog message will be sent and/or the VLAN is moved to the blocked state when the action is violated.
<b>notification</b>	(Optional) Specifies the type of notification to be sent when the action is violated.
<b>syslog</b>	Sends a syslog message when the action is violated.
<b>trap</b>	Sends trap notifications when the action is violated.
<b>both</b>	Sends syslog and trap notifications when the action is violated.
<b>vlan vlan</b>	(Optional) Enables MAC limiting on a per-VLAN basis.
<b>interface type mod/port</b>	(Optional) Enables MAC limiting on a per-port basis.
<b>flood</b>	(Optional) Enables unknown unicast flooding on a VLAN.

### Defaults

The defaults are as follows:

- **maximum num** is **500** MAC address entries.
- **action** is **warning**.
- **notification** is **syslog**.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

Use this syntax for enabling MAC limiting globally:

```
mac-address-table limit [maximum num] [action {warning | limit | shutdown}]
[notification {syslog | trap | both}]
```

Use this syntax for enabling per-VLAN MAC limiting:

```
mac-address-table limit [vlan vlan] [maximum num] [action {warning | limit | shutdown}]
[flood]
```

Use this syntax for enabling per-port MAC limiting:

```
mac-address-table limit [interface type mod/port] [maximum num] [action {warning | limit |
shutdown}] [flood]
```

If you enable per-VLAN MAC limiting, the per-VLAN MAC limiting supersedes the **mac-address-table limit** command that globally enables MAC limiting.

The maximum number of MAC entries is based per VLAN and per EARL.

If you do not specify a maximum, an action, or a notification, the default settings are used.

If you enable per-VLAN MAC limiting, MAC limiting is enabled on the VLAN specified only.

The **flood** keyword is supported on VLAN interfaces only.

The **flood** action occurs only if the **limit** action is configured and is violated.

In the **shutdown** state, the VLAN remains in the blocked state until you reenables it through the CLI.

**Examples**

This example shows how to enable the MAC limit globally:

```
Router(config)# mac-address-table limit
Router(config)#
```

This example shows how to enable per-VLAN MAC limiting:

```
Router(config)# mac-address-table limit vlan 501 maximum 50 action shutdown
Router(config)#
```

**Related Commands**

Command	Description
<a href="#">show mac-address-table limit</a>	Displays the information about the MAC-address table.

## mac-address-table notification mac-move

To enable MAC-move notification, use the **mac-address-table notification mac-move** command. To disable MAC-move notification, use the **no** form of this command.

**mac-address-table notification mac-move**

**no mac-address-table notification mac-move**

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

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

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** MAC-move notification generates a syslog message whenever a MAC address or host moves between different switch ports.

MAC-move notification does not generate a notification when a new MAC address is added to the CAM or when a MAC address is removed from the CAM.

MAC-move notification is supported on switch ports only.

**Examples** This example shows how to enable MAC-move notification:

```
Router(config)# mac-address-table notification mac-move
Router(config)#
```

This example shows how to disable MAC-move notification:

```
Router(config)# no mac-address-table notification mac-move
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show mac-address-table notification mac-move</a>	Displays the information about the MAC-address table.

# mac-address-table notification threshold

To enable CAM table usage monitoring notification, use the **mac-address-table notification threshold** command. To disable CAM table usage monitoring notification, use the **no** form of this command.

**mac-address-table notification threshold** {*limit percentage*} {*interval time*}

**no mac-address-table notification threshold**

Syntax Description	limit <i>percentage</i>	interval <i>time</i>
	Specifies the percentage of the CAM utilization; valid values are from 1 to 100 percent.	Specifies the time between notifications; valid values are greater than or equal to 120 seconds.

## Defaults

The defaults are as follows:

- Disabled.
- *percentage* is **50** percent.
- *time* is **120** seconds.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

When you enable CAM table usage monitoring, the number of valid entries in the CAM table are counted and if the percentage of the CAM utilization is higher or equal to the specified threshold, a message is displayed.

## Examples

This example shows how to enable CAM table usage monitoring notification and use the default settings:

```
Router(config)# mac-address-table notification threshold
Router(config)#
```

This example shows how to enable CAM table usage monitoring notification and set the threshold and interval:

```
Router(config)# mac-address-table notification threshold limit 20 interval 200
Router(config)#
```

## ■ mac-address-table notification threshold

This example shows how to disable CAM table usage monitoring notification:

```
Router(config)# no mac-address-table notification threshold
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show mac-address-table notification threshold</a>	Displays information about the MAC-address table.

## mac-address-table static

To add static entries to the MAC-address table or configure a static MAC address with IGMP snooping disabled for that address, use the **mac-address-table static** command. See the “Usage Guidelines” section for information about the **no** form of this command.

```
mac-address-table static mac-addr vlan vlan-id {interface type | drop [disable-snooping]}
[dcli dcli | pvc vpi/vci] [auto-learn | disable-snooping] [protocol {ip | ipv6 | ipx | assigned}]
```

```
no mac-address-table static mac-addr {vlan vlan-id} {interface type} [disable-snooping] [dcli
dcli | pvc vpi/vci]
```

Syntax Description		
<i>mac-addr</i>		Address to add to the MAC-address table.
<b>vlan</b> <i>vlan-id</i>		Specifies the VLAN to apply the changed aging time; valid values are from 1 to 4094.
<b>interface</b> <i>type</i>		Specifies the interface type and module/port number.
<b>drop</b>		Drops all traffic that is received from and going to the configured MAC address in the specified VLAN.
<b>disable-snooping</b>	(Optional)	Disables IGMP snooping on the multicast MAC address.
<b>dcli</b> <i>dcli</i>	(Optional)	Specifies mapping the DLCI to this MAC address; valid values are from 16 to 1007.
<b>pvc</b> <i>vpi/vci</i>	(Optional)	Specifies mapping the PVC to this MAC address.
<b>auto-learn</b>	(Optional)	Updates the entry with the new port; see the “Usage Guidelines” section for additional information.
<b>protocol</b>	(Optional)	Specifies the protocol that is associated with the entry.
<b>ip</b>		Specifies the IP protocol.
<b>ipv6</b>		Specifies the IPv6 protocol.
<b>ipx</b>		Specifies the IPX protocol.
<b>assigned</b>		Specifies assigned protocol bucket accounts for such protocols as DECnet, Banyan VINES, and AppleTalk.

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

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Use the **no** form of this command to do the following:

- Remove entries that are profiled by the combination of specified entry information.

- Note that IGMP snooping is not disabled for the specified address.
- Remove the MAC address to a Frame Relay DLCI or ATM PVC mapping.

The **dlci** *dlci* keyword and argument are valid only if Frame Relay encapsulation has been enabled on the specified interface.

The **pvc** *vpi/vci* keyword and arguments are supported on ATM interfaces only.

When specifying the **pvc** *vpi/vci*, you must specify both a VPI and a VCI, separated by a slash.

When you install a static MAC address, it is associated with a port. If the same MAC address is seen on a different port, the entry is updated with the new port if you enter the **auto-learn** keyword.

The output interface specified must be a Layer 2 IDB and not an SVI.

The **ipx** keyword is not supported.

You can enter up to 15 interfaces per command entered, but you can enter more interfaces by repeating the command.

If you do not enter a protocol type, an entry is automatically created for each of the four protocol types.

Entering the **no** form of this command does not remove system MAC addresses.

When removing a MAC address, entering **interface** *type* is optional. For unicast entries, the entry is removed automatically. For multicast entries, if you do not specify an interface, the entire entry is removed. You can specify the selected ports to be removed by specifying the interface.

The **mac-address-table static** *mac-addr* {**vlan** *vlan-id*} {**interface** *type*} **disable-snooping** command disables snooping on the specified static MAC entry/VLAN pair only. To reenabling snooping, you must first delete the MAC address and then reinstall it using the **mac-address-table static** *mac-addr* {**vlan** *vlan-id*} {**interface** *type*} command without entering the **disable-snooping** keyword.

The **mac-address-table static** *mac-addr* {**vlan** *vlan-id*} **drop** command cannot be applied to a multicast MAC address.

To support multipoint bridging and other features, you must also specify the **dlci** *dlci* keyword and argument for Frame Relay interfaces or the **pvc** *vpi/vci* keyword and arguments for ATM interfaces as follows:

```
Router(config)# mac-address-table static 000C.0203.0405 vlan 101 interface ATM6/1 pvc6/101
Router(config)#
```



#### Note

If you omit the **dlci** *dlci* keyword and argument for Frame Relay interfaces, the MAC address is mapped to the first DLCI circuit that is configured for the specified VLAN on that interface. If you omit the **pvc** *vpi/vci* keyword and arguments for ATM interfaces, the MAC address is mapped to the first PVC circuit that is configured for the specified VLAN on that interface. To ensure that the MAC address is configured correctly, we recommend that you always use the **dlci** *dlci* and **pvc** *vpi/vci* keywords and arguments on the appropriate interfaces.

#### Examples

This example shows how to add static entries to the MAC-address table:

```
Router(config)# mac-address-table static 0050.3e8d.6400 vlan 100 interface fastethernet5/7
Router(config)#
```

This example shows how to configure a static MAC address with IGMP snooping disabled for a specified address:

```
Router(config)# mac-address-table static 0050.3e8d.6400 vlan 100 interface fastethernet5/7 disable-snooping
Router(config)#
```

This example shows how to add static entries to the MAC address table for an ATM PVC circuit and for a Frame Relay DLCI circuit:

```
Router(config)# mac-address-table static 0C01.0203.0405 vlan 101 interface ATM6/1 pvc 6/101
Router(config)# mac-address-table static 0C01.0203.0406 vlan 202 interface POS4/2 dlc1 200
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show mac-address-table</a>	Displays information about the MAC-address table.

# mac-address-table synchronize

To synchronize the Layer 2 MAC address table entries across the PFC and all the DFCs, use the **mac-address-table synchronize** command. To disable MAC address table synchronization or reset the activity timer, use the **no** form of this command.

**mac-address-table synchronize** [**activity-time** *seconds*]

**no mac-address-table synchronize** [**activity-time** *seconds*]

## Syntax Description

**activity-time** *seconds* (Optional) Specifies the activity timer interval: valid values are **160**, **320**, and **640** seconds.

## Defaults

The default settings are as follows:

- Disabled.
- Enabled for WS-X6708-10GE.
- **activity-time** is 160 seconds.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

We recommend that you configure the activity time so that at least two activity times exist within the regular Layer 2 aging time (or within the aging time used for VLANs in distributed EtherChannels if this feature is used only for distributed EtherChannels). If at least two activity times do not exist within the aging time, then an error message is displayed.

## Examples

This example shows how to specify the activity timer interval:

```
Router(config)# mac-address-table synchronize activity-time 320
Router(config)#
```

## Related Commands

Command	Description
<b>show mac-address-table synchronize statistics</b>	Displays information about the MAC-address table.

# mac packet-classify

To classify Layer 3 packets as Layer 2 packets, use the **mac packet-classify** command. To return to the default settings, use the **no** form of this command.

**mac packet-classify**

**no mac packet-classify**

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

**Defaults** Disabled

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** PFC3BXL and PFC3B modes support protocol-independent MAC ACL filtering. Protocol-independent MAC ACL filtering applies MAC ACLs to all ingress traffic types (for example, IPv4 traffic, IPv6 traffic, and MPLS traffic, in addition to MAC-layer traffic).

You can configure these interface types for multilayer MAC ACL QoS filtering:

- VLAN interfaces without Layer 3 addresses
- Physical LAN ports that are configured to support EoMPLS
- Logical LAN subinterfaces that are configured to support EoMPLS

The ingress traffic that is permitted or denied by a MAC ACL on an interface configured for multilayer MAC ACL QoS filtering is processed by egress interfaces as MAC-layer traffic. You cannot apply egress IP ACLs to traffic that was permitted or denied by a MAC ACL on an interface configured for multilayer MAC ACL QoS filtering.

Microflow policing does not work on interfaces that have the **mac packet-classify** command enabled.

The **mac packet-classify** command causes the Layer 3 packets to be classified as Layer 2 packets and disables IP classification.

Traffic is classified based on 802.1Q CoS, trunk VLAN, EtherType, and MAC addresses.

**Examples** This example shows how to classify incoming and outgoing Layer 3 packets as Layer 2 packets:

```
Router(config-if)# mac packet-classify
Router(config-if)#
```

■ `mac packet-classify`

This example shows how to disable the classification of incoming and outgoing Layer 3 packets as Layer 2 packets:

```
Router(config-if)# no mac packet-classify
Router(config-if)#
```

## Related Commands

Command	Description
<a href="#">mac packet-classify</a>	Enables VLAN-based QoS filtering in the MAC ACLs.
<a href="#">use vlan</a>	

# mac packet-classify use vlan

To enable VLAN-based QoS filtering in the MAC ACLs, use the **mac packet-classify use vlan** command. To return to the default settings, use the **no** form of this command.

**mac packet-classify use vlan**

**no mac packet-classify use vlan**

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

**Defaults** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** PFC3BXL and PFC3B modes support protocol-independent MAC ACL filtering. Protocol-independent MAC ACL filtering applies MAC ACLs to all ingress traffic types (for example, IPv4 traffic, IPv6 traffic, and MPLS traffic, in addition to MAC-layer traffic).

You must use the **no mac packet-classify use vlan** command to disable the VLAN field in the Layer 2 key if you want to apply QoS to the Layer 2 SAP-encoded packets (for example, IS-IS and IPX).

QoS does not allow policing of non-ARPA Layer 2 packets (for example, IS-IS and IPX) if the VLAN field is enabled.

**Examples** This example shows how to enable VLAN-based QoS filtering in the MAC ACLs:

```
Router(config)# mac packet-classify use vlan
Router(config)
```

This example shows how to disable VLAN-based QoS filtering in the MAC ACLs:

```
Router(config)# no mac packet-classify use vlan
Router(config)
```

Related Commands	Command	Description
	<a href="#">mac packet-classify</a>	Classifies Layer 3 packets as Layer 2 packets.

# match

To specify the match clause by selecting one or more ACLs for a VLAN access-map sequence, use the **match** subcommand. The match clause specifies the IP, IPX, or MAC ACLs for traffic filtering. To remove the match clause, use the **no** form of this command.

```
match {ip address {acl-number | acl-name}} | {ipx address {acl-number | acl-name}} | {mac address acl-name}}
```

```
no match {ip address {acl-number | acl-name}} | {ipx address {acl-number | acl-name}} | {mac address acl-name}}
```

## Syntax Description

<b>ip address</b> <i>acl-number</i>	Selects one or more IP ACLs for a VLAN access-map sequence; valid values are from 1 to 199 and from 1300 to 2699.
<b>ip address</b> <i>acl-name</i>	Selects an IP ACL by name.
<b>ipx address</b> <i>acl-number</i>	Selects one or more IPX ACLs for a VLAN access-map sequence; valid values are from 800 to 999.
<b>ipx address</b> <i>acl-name</i>	Selects an IPX ACL by name.
<b>mac address</b> <i>acl-name</i>	Selects one or more MAC ACLs for a VLAN access-map sequence.

## Defaults

This command has no default settings.

## Command Modes

VLAN access-map submenu

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

The **match ip address** and **match mac address** commands are not supported for VACLs on WAN interfaces.

IPX ACLs that are used in VACLs can only specify the IPX protocol type, the source network, the destination network, and the destination host address.

The MAC sequence is not effective for IP or IPX packets. IP packets and IPX packets should be access controlled by IP and IPX match clauses.

You cannot configure VACLs on secondary VLANs. The secondary VLAN inherits all features that are configured on the primary VLAN.

These subcommands appear in the CLI help but are not supported by the PFC QoS:

- **match cos**
- **match any**
- **match class-map**
- **match destination-address**

- **match input-interface**
- **match qos-group**
- **match source-address**

Refer to the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY* for additional configuration guidelines and restrictions.

Refer to the *Cisco IOS Release 12.2 Command Reference* publication for additional **match** command information.

### Examples

This example shows how to define a match clause for a VLAN access map:

```
Router(config)# vlan access-map ganymede 10
Router(config-access-map)# match ip address 13
Router(config-access-map)#
```

### Related Commands

Command	Description
<a href="#">action</a>	Sets the packet action clause.
<a href="#">port access-map</a>	Creates a port access map or enters port access-map command mode.
<a href="#">show vlan access-map</a>	Displays the contents of a VLAN-access map.
<a href="#">vlan access-map</a>	Creates a VLAN access map or enters VLAN access-map command mode.

# match protocol

To configure the match criteria for a class map on the basis of the specified protocol, use the **match protocol** command. To remove the protocol-based match criteria from a class map, use the **no** form of this command.

```
match protocol {ip | ipv6}
```

```
no match protocol {ip | ipv6}
```

Syntax Description	<b>ip</b>	Specifies protocol matching on IP packets.
	<b>ipv6</b>	Specifies protocol matching on IPv6 packets.

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

**Command Modes** Class-map submode

**Command History**

12.2(18)ZY	Support for this command was introduced.
------------	--

**Usage Guidelines** The **match protocol** class-map subcommand configures NBAR and sends all traffic on the port, both ingress and egress, to be processed in the software on the PISA.

For class-based weighted fair queueing, you define traffic classes based on match criteria including protocols, ACLs, input interfaces, QoS labels, and EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **match protocol** command specifies the name of a protocol to be used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

To use the **match protocol** command, you must first enter the **class-map** command to specify the name of the class to which you want to establish the match criteria.

If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

This command can be used to match protocols that are known to the NBAR feature. For a list of protocols currently supported by NBAR, see the “Classification” section of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

**Examples** This example shows how to specify a class map called ip and configure the IP as a match criterion for it:

```
Router(config)# class-map ip
Router(config-cmap)# match protocol ip
```

## maxconns (real server configuration submode)

To limit the number of active connections to the real server, use the **maxconns** command. To change the maximum number of connections to the default settings, use the **no** form of this command.

**maxconns** *number-conns*

**no maxconns**

<b>Syntax Description</b>	<i>number-conns</i> Maximum number of active connections on the real server at any one point in time; valid values are from 0 to 4294967295.
---------------------------	--

<b>Defaults</b>	0
-----------------	---

<b>Command Modes</b>	Real server configuration submode
----------------------	-----------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	If you do not specify the <i>number-conns</i> value, the default value is <b>0</b> , which means that the maximum number of connections to the real server are not monitored.
-------------------------	---

<b>Examples</b>	This example shows how to limit the number of active connections to the real server:
-----------------	--

```
Router(config-if)# maxconns 49672
Router(config-if)#
```

This example shows how to revert to the default settings:

```
Router(config-if)# no maxconns
Router(config-if)#
```

Related Commands	Command	Description
	<b>faildetect numconns</b>	Specifies the conditions that indicate a server failure.
	<b>inservice (real server)</b>	Enables the real server for use by the Cisco IOS SLB feature.
	<b>reassign</b>	Defines the number of consecutive number of SYNs for a new connection that will go unanswered before the connection is attempted to a different real server.
	<b>retry</b>	Defines the amount of time that must elapse before a connection is attempted to a failed server.

# maximum-paths

To control the maximum number of parallel routes that an IP routing protocol can support, use the **maximum-paths** command. To restore the default settings, use the **no** form of this command.

**maximum-paths** *maximum*

**no maximum-paths**

<b>Syntax Description</b>	<i>maximum</i> Maximum number of parallel routes that an IP routing protocol installs in a routing table; valid values are from 1 to 8.
---------------------------	---

<b>Defaults</b>	<p>The defaults are as follows:</p> <ul style="list-style-type: none"> <li>• BGP has one path.</li> <li>• All other IP routing protocols have four paths.</li> </ul>
-----------------	--

<b>Command Modes</b>	Routing protocol configuration
----------------------	--------------------------------

<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(18)ZY</td> <td>Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)ZY	Support for this command was introduced.
Release	Modification				
12.2(18)ZY	Support for this command was introduced.				

<b>Examples</b>	<p>This example shows how to allow a maximum of two paths to a destination:</p> <pre>Router(config-router)# <b>maximum-paths 2</b> Router(config-router)</pre>
-----------------	--

## mdix auto

To enable automatic media-dependent interface with crossover detection, use the **mdix auto** command. To turn automatic detection off, use the **no** form of this command.

**mdix auto**

**no mdix auto**

---

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

---

**Defaults** Enabled

---

**Command Modes** EXEC

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Usage Guidelines** This command is supported on the following modules only:

- WS-X6748-GE-TX
- WS-SUP720 (copper ports only)
- WS-SUP720-10G (copper ports only)
- WS-SUP32 (copper ports only)
- WS-X6148A-RJ45
- WS-X6148A-GE-TX
- WS-X6548-RJ45
- WS-X6548-RJ21
- WS-X6548-GE-TX
- WS-X6516-GE-TX
- WS-X6148-GE-TX
- WS-X6148X2-RJ45
- WS-X6196-RJ21
- The copper SFP (GLC-T) and the copper GBIC (WS-G5483) also support automatic MDIX when used in one of the modules that support these transceivers.

---

**Examples**

This example shows how to enable automatic media-dependent interface with crossover detection:

```
Router# mdix auto  
Router#
```

This example shows how to disable automatic media-dependent interface with crossover detection:

```
Router# no mdix auto  
Router#
```

## mdt data

To configure the multicast group address range for data MDT groups, use the **mdt data** command. To disable this function, use the **no** form of this command.

**mdt data** *group-address-range wildcard-bits* [**threshold** *threshold-value*] [**list** *access-list*]

**no mdt data** *group-address-range wildcard-bits* [**threshold** *threshold-value*] [**list** *access-list*]

Syntax Description	
<i>group-address-range</i>	Multicast group address range; valid values are from 224.0.0.1 to 239.255.255.255.
<i>wildcard-bits</i>	Wildcard bits to be applied to the multicast group address range.
<b>threshold</b> <i>threshold-value</i>	(Optional) Defines the bandwidth threshold value; valid values are from 1 through 4294967.
<b>list</b> <i>access-list</i>	(Optional) Defines the access-list name or number.

**Defaults** Disabled

**Command Modes** VRF configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

A data MDT group can include a maximum of 256 multicast groups per VPN. Multicast groups that are used to create the data MDT group are dynamically chosen from a pool of configured IP addresses.

This command configures a range of alternative multicast destination addresses for the tunnel header. The destination address chosen depends on the traffic profile (the source and destination match the specified access list and the rate of the traffic has exceeded the bandwidth threshold value).

**Examples** This example shows how to configure the multicast group address range for data MDT groups:

```
Router(config-vrf)# mdt data 232.0.1.0 0.0.0.255 threshold 500 list 101
Router(config-vrf)#
```

Related Commands	Command	Description
	<b>mdt default</b>	Configures a default MDT group for a VRF instance.

## mdt default

To configure a default MDT group for a VRF instance, use the **mdt default** command in VRF configuration mode. To disable this function, use the **no** form of this command.

**mdt default** *group-address*

**no mdt default** *group-address*

Syntax	Description
<i>group-address</i>	IP address of the default MDT group.

Defaults	Description
	Disabled

Command Modes	Description
	VRF configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Usage Guidelines	Description
	The default MDT group must be the same group that is configured on all provider-edge routers that belong to the same VPN.
	The <i>group-address</i> serves as an identifier for the community because provider-edge routers that are configured with the same group address become members of the group, allowing them to receive packets that are sent by each other.
	If you use the SSM protocol for the default MDT, the source IP address is used to source the BGP sessions.
	A tunnel interface is created when you enter this command. By default, the destination address of the tunnel header is the <i>group-address</i> argument.

Examples	Description
	This example shows how to configure a default MDT group for a VRF instance:

```
Router(config-vrf)# mdt default 232.0.0.1
Router(config-vrf)#
```

Related Commands	Command	Description
	<a href="#">mdt data</a>	Configures the multicast group address range for data MDT groups.

## mdt log-reuse

To enable the recording of data MDT reuse, use the **mdt log-reuse** command in VRF configuration mode. To disable this function, use the **no** form of this command.

**mdt log-reuse**

**no mdt log-reuse**

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

**Defaults** Disabled

**Command Modes** VRF configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **mdt log-reuse** command generates a syslog message whenever a data MDT is reused.

**Examples** This example shows how to enable the MDT log reuse function:

```
Router(config-vrf)# mdt log-reuse
Router(config-vrf)#
```

Related Commands	Command	Description
	<a href="#">mdt data</a>	Configures the multicast group address range for data MDT groups.
	<a href="#">mdt default</a>	Configures a default MDT group for a VRF instance.

# media-type

To select the connector to use for the dual-mode uplink port, use the **media-type** command. To return to the default settings, use the **no** form of this command.

**media-type {rj45 | sfp}**

**no media-type**

Syntax Description	Command	Description
	<b>rj45</b>	Uses an RJ-45 connector.
	<b>sfp</b>	Uses an SFP connector.

**Defaults** **sfp**

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

Port 1 has a small form-factor pluggable (SFP) connector.

Port 2 has an RJ-45 connector and an SFP connector. You must configure the port to use one connector or the other.

**Examples** This example shows how to configure port 2 in slot 5 to use the RJ-45 connector:

```
Router(config)# interface gigabitethernet 5/2
Router(config-if)# media-type rj45
```

## mkdir disk0:

To create a new directory in a flash file system, use the **mkdir disk0:** command.

### **mkdir disk0:**

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

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command is valid only on flash file systems.

After you enter the **mkdir disk0:** command, you are prompted to enter the new directory filename.

To check your entry, enter the **dir** command.

To remove a directory, enter the **rmdir** command.

**Examples** This example shows how to create a directory named newdir:

```
Router# mkdir disk0:
Create directory filename [ ]? newdir
Created dir disk0: newdir
Router#
```

Related Commands	Command	Description
	<b>cd</b>	Changes the default directory or file system.
	<b>dir</b>	Displays a list of files on a file system.
	<b>rmdir</b>	Removes an existing directory in a Class C flash file system.

# mls aclmerge algorithm

To select the type of ACL merge method to use, use the **mls aclmerge algorithm** command.

```
mls aclmerge algorithm {bdd | odm }
```

Syntax Description	bdd	Specifies the BDD-based algorithm.
	odm	Specifies the ODM-based algorithm.

Defaults	<b>bdd</b>
----------	------------

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The BDD-based ACL merge uses Boolean functions to condense entries into a single merged list of TCAM entries that can be programmed into the TCAM.

You cannot disable the ODM-based ACL merge on Catalyst 6500 series switches.

The ODM-based ACL merge uses an order-dependent merge algorithm to process entries that can be programmed into the TCAM.



**Note**

The ODM-based ACL merge supports both security ACLs and ACLs that are used for QoS filtering.

If you change the algorithm method, the change is not retroactive. For example, ACLs that have had the merge applied are not affected. The merge change applies to future merges only.

Use the [show fm summary](#) command to see the status of the current merge method.

## Examples

This example shows how to select the BDD-based ACL to process ACLs:

```
Router(config)# mls aclmerge algorithm bdd
The algorithm chosen will take effect for new ACLs which are being applied, not
for already applied ACLs1
Router(config)
```

This example shows how to select the ODM-based ACL merge to process ACLs:

```
Router(config)# mls aclmerge algorithm odm
The algorithm chosen will take effect for new ACLs which are being applied, not
for already applied ACLs1
Router(config)#
```

■ mls aclmerge algorithm

Related Commands	Command	Description
	<a href="#">show fm summary</a>	Displays a summary of feature manager information.

## mls acl tcam default-result

To set the default action during the ACL TCAM update, use the **mls acl tcam default-result** command. To return to the default settings, use the **no** form of this command.

```
mls acl tcam default-result {permit | deny | bridge}
```

```
no mls acl tcam default-result
```

Syntax Description	Command	Description
	<b>permit</b>	Permits all traffic.
	<b>deny</b>	Denies all traffic.
	<b>bridge</b>	Bridges all Layer 3 traffic up to the rendezvous point.

**Defaults** **deny**

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** In the transition time between when an existing ACL is removed and a new ACL is applied, a default **deny** is programmed in the hardware. Once the new ACL has been applied completely in the hardware, the default **deny** is removed.

Use the **mls acl tcam default-result permit** command to permit all traffic in the hardware or bridge all traffic to the software during the transition time.

**Examples** This example shows how to permit all traffic to pass during the ACL TCAM update:

```
Router(config)# mls acl tcam default-result permit
Router(config)#
```

This example shows how to deny all traffic during the ACL TCAM update:

```
Router(config)# mls acl tcam default-result deny
Router(config)#
```

This example shows how to bridge all Layer 3 traffic up to the rendezvous point during the ACL TCAM update:

```
Router(config)# mls acl tcam default-result bridge
Router(config)#
```

## mls acl tcam share-global

To enable sharing of the global default ACLs, use the **mls acl tcam share-global** command. To turn off sharing of the global defaults, use the **no** form of this command.

**mls acl tcam share-global**

**no mls acl tcam share-global**

---

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

---

**Defaults** Enabled

---

**Command Modes** Global configuration

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Examples** This example shows how to enable sharing of the global default ACLs:

```
Router(config)# mls acl tcam share-global
Router(config)#
```

## mls aging fast

To configure the fast-aging time for unicast entries in the Layer 3 table, use the **mls aging fast** command. To restore the MLS fast-aging time to the default settings, use the **no** form of this command.

```
mls aging fast [{threshold packet-count} [{time seconds}]]
```

```
mls aging fast [{time seconds} [{threshold packet-count}]]
```

```
no mls aging fast
```

Syntax Description	
<b>threshold</b>	(Optional) Specifies the packet count of the fast-aging threshold for <i>packet-count</i> Layer 3 fast aging; valid values are from 1 to 128.
<b>time seconds</b>	(Optional) Specifies how often entries are checked; valid values are from 1 to 128 seconds.

### Defaults

The defaults are as follows:

- Fast aging is disabled.
- If fast aging is enabled, the default *packet-count* value is 100 packets and the *seconds* default is 32 seconds.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

This command has no effect when you configure sampled NetFlow. You must disable sampled NetFlow to allow this command to take effect.

### Examples

This example shows how to configure the MLS fast-aging threshold:

```
Router(config)# mls aging fast threshold 50
Router(config)#
```

### Related Commands

Command	Description
<a href="#">show mls netflow</a>	Displays configuration information about the NetFlow hardware.

## mls aging long

To configure the long-aging time for unicast entries in the Layer 3 table, use the **mls aging long** command. To restore the MLS long-aging time to the default settings, use the **no** form of this command.

**mls aging long** *seconds*

**no mls aging long**

<b>Syntax Description</b>	<i>seconds</i> Layer 3 long-aging timeout; valid values are from 64 to 1920 seconds.
---------------------------	--

<b>Defaults</b>	<b>1920</b> seconds
-----------------	---------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	This command has no effect when you configure sampled NetFlow. You must disable sampled NetFlow to allow this command to take effect.
-------------------------	---

<b>Examples</b>	This example shows how to configure the MLS long-aging threshold:
-----------------	---

```
Router(config)# mls aging long 800
Router(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show mls netflow</a>	Displays configuration information about the NetFlow hardware.

# mls aging normal

To configure the normal-aging time for unicast entries in the Layer 3 table, use the **mls aging normal** command. To restore the MLS normal-aging time to the default settings, use the **no** form of this command.

**mls aging normal** *seconds*

**no mls aging normal**

<b>Syntax Description</b>	<i>seconds</i>	Normal aging timeout for Layer 3; valid values are from 32 to 4092 seconds.				
<b>Defaults</b>	<b>300</b>	seconds				
<b>Command Modes</b>	Global configuration					
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(18)ZY</td> <td>Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)ZY	Support for this command was introduced.	
Release	Modification					
12.2(18)ZY	Support for this command was introduced.					
<b>Usage Guidelines</b>	This command has no effect when you configure sampled NetFlow. You must disable sampled NetFlow to allow this command to take effect.					
<b>Examples</b>	<p>This example shows how to configure the MLS normal-aging threshold:</p> <pre>Router(config)# mls aging normal 200 Router(config)#</pre>					
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><a href="#">show mls netflow</a></td> <td>Displays configuration information about the NetFlow hardware.</td> </tr> </tbody> </table>	Command	Description	<a href="#">show mls netflow</a>	Displays configuration information about the NetFlow hardware.	
Command	Description					
<a href="#">show mls netflow</a>	Displays configuration information about the NetFlow hardware.					

## mls cef maximum-routes

To limit the maximum number of the routes that can be programmed in the hardware allowed per protocol, use the **mls cef maximum-routes** command. To return to the default settings, use the **no** form of this command.

```
mls cef maximum-routes {ip maximum-routes} | {ip-multicast maximum-routes} |
  {ipv6 maximum-routes} | {mpls maximum-routes}
```

```
no mls cef maximum-routes {ip | ip-multicast | ipv6 | mpls}
```

Syntax Description	ip	ip-multicast	ipv6	mpls
	Specifies the maximum number of IP routes.			
	<i>maximum-routes</i>			
		Specifies the maximum number of multicast routes.		
			Specifies the maximum number of IPv6 routes.	
				Specifies the maximum number of MPLS labels.

### Defaults

The defaults are as follows:

- For XL-mode systems:
  - IPv4 unicast and MPLS—512,000 routes
  - IPv6 multicast/unicast and IPv4 multicast—256,000 routes
- For non-XL mode systems:
  - IPv4 unicast and MPLS—192,000 routes
  - IPv6 multicast/unicast and IPv4 multicast—32,000 routes



#### Note

The size of the global Internet routing table plus any local routes might exceed the non-XL mode default partition sizes. See the “Usage Guidelines” section for additional information.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

---

**Usage Guidelines****Note**

If you copy a configuration file that contains the MLS CEF maximum routes into the startup-config file and reload the Catalyst 6500 series switch, the Catalyst 6500 series switch reloads after it reboots.

The **mls cef maximum-routes** command limits the maximum number of the routes that can be programmed in the hardware. If routes are detected that exceed the limit for that protocol, an exception condition is generated.

The XL and non-XL modes are based on the type of PFC module that is installed in your system. You cannot configure the mode except by the installed hardware. The Supervisor Engine 32 PISA contains a PFC3B and is considered a non-XL mode system.

The valid values for *max-routes* are as follows:

- IP and MPLS— Up to 239,000 routes
- IP-multicast and IPv6 multicast/unicast—Up to 119,000 routes

**Note**

The maximum values that you are permitted to configure is not fixed but varies depending on the values that are allocated for other protocols.

An example of how to enter the maximum routes argument is as follows:

```
Router(config)# mls cef maximum-routes ip 4
```

where 4 is 4096 IP routes (1024 x4 = 4096).

The new configurations are applied after a system reload only and do not take effect if a switchover occurs.

In RPR mode, if you change and save the maximum-routes configuration, the redundant supervisor engine reloads when it becomes active from either a switchover or a system reload. The reload occurs 5 minutes after the supervisor engine becomes active.

Use the **show mls cef maximum-routes** command to view the current maximum routes system configuration.

---

**Examples**

This example shows how to set the maximum number of routes that are allowed per protocol:

```
Router(config)# mls cef maximum-routes ip 100
Router(config)#
```

This example shows how to return to the default setting for a specific protocol:

```
Router(config)# no mls cef maximum-routes ip
Router(config)#
```

---

**Related Commands**

Command	Description
<b>show mls cef maximum-routes</b>	Displays the current maximum-route system configuration.

# mls cef tunnel fragment

To allow tunnel fragmentation, use the **mls cef tunnel fragment** command. To return to the default settings, use the **no** form of this command.

**mls cef tunnel fragment**

**no mls cef tunnel fragment**

---

**Defaults** Disabled

---

**Command Modes** Global configuration

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Usage Guidelines** When you enable tunnel fragmentation, if the size of the packets that are going into a tunnel interface exceed the MTU, the packet is fragmented. The packets that are fragmented are reassembled at the destination point.

---

**Examples** This example shows how to allow tunnel fragmentation:

```
Router(config)# mls cef tunnel fragment
Router(config)#
```

This example shows how to return to the default setting:

```
Router(config)# no mls cef tunnel fragment
Router(config)#
```

---

Related Commands	Command	Description
	<b>show mls cef tunnel fragment</b>	Displays the operational status of tunnel fragmentation.

---

## mls erm priority

To assign the priorities to define an order in which protocols attempt to recover from the exception status, use the **mls erm priority** command. To return to the default settings, use the **no** form of this command.

```
mls erm priority {ipv4 value} {ipv6 value} {mpls value}
```

```
no mls erm priority {ipv4} {ipv6} {mpls}
```

Syntax Description		
<b>ipv4</b>		Prioritizes the IPv4 protocol.
<i>value</i>		Priority value; valid values are from 1 to 3.
<b>ipv6</b>		Prioritizes the IPv6 protocol.
<b>mpls</b>		Prioritizes the MPLS protocol.

**Defaults** The default settings are as follows:

- **ipv4** is **1**.
- **ipv6** is **2**.
- **mpls** is **3**.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** A lower *value* indicates a higher priority.

When a protocol sees a FIB table exception, the protocol notifies the FIB ERM manager. The FIB ERM manager periodically polls the FIB table exception status and decides which protocol gets priority over another protocol when multiple protocols are running under the exception. Only one protocol can attempt to recover from an exception at any time.

If there is sufficient FIB space, the protocol with the highest priority tries to recover first. Other protocols under the exception do not start to recover until the previous protocol completes the recovery process by reloading the appropriate FIB table.

---

**Examples**

This example shows how to set the ERM exception-recovery priority:

```
Router(config)# mls erm priority ipv4 1 ipv6 2 mpls 3
Router(config)#
```

This example shows how to return to the default setting:

```
Router(config)# no mls erm priority ipv4 ipv6 mpls
Router(config)#
```

---

**Related Commands**

Command	Description
<a href="#">show mls cef exception</a>	Displays information about the CEF exception.

# mls exclude protocol

To specify the interface protocol to exclude from shortcutting, use the **mls exclude protocol** command. To remove a prior entry, use the **no** form of this command.

```
mls exclude protocol {{ both | tcp | udp } { port port-number }
```

```
no mls exclude
```

Syntax	Description
<b>both</b>	Specifies both UDP and TCP.
<b>tcp</b>	Excludes TCP interfaces from shortcutting.
<b>udp</b>	Specifies UDP interfaces from shortcutting.
<b>port</b> <i>port-number</i>	Specifies the port number; valid values are from 1 to 65535.

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

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to configure MLS to exclude UDP on port 69:

```
Router(config)# mls exclude protocol udp port 69
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show mls ip multicast</a>	Displays the MLS IP information.

■ mls exclude protocol

# mls flow

To configure the flow mask for NDE, use the **mls flow** command. To restore the flow mask to the default, use the **no** form of this command.

```
mls flow {{ip | ipv6} {destination | destination-source | full | interface-destination-source |
interface-full | source}}
```

```
no mls flow {ip | ipv6}
```

## Syntax Description

<b>ip</b>	Enables the flow mask for MLS IP packets.
<b>ipv6</b>	Enables the flow mask for MLS IPv6 packets.
<b>destination</b>	Uses the destination IP address as the key to the Layer 3 table.
<b>destination-source</b>	Uses the destination and the source IP address as the key to the Layer 3 table.
<b>full</b>	Uses the source and destination IP address, the IP protocol (UDP or TCP), and the source and destination port numbers as the keys to the Layer 3 table.
<b>interface-destination-source</b>	Uses all the information in the destination and source flow mask and the source VLAN number as the keys to the Layer 3 table.
<b>interface-full</b>	Uses all the information in the full flow mask and the source VLAN number as the keys to the Layer 3 table.
<b>source</b>	Uses all the information in the source flow mask only.

## Defaults

The NDE flow mask is null.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

This command collects statistics for the supervisor engine.

## Examples

This example shows how to set the minimum flow mask for an extended access list for MLS IP:

```
Router(config)# mls flow ip full
Router(config)#
```

## Related Commands

Command	Description
<a href="#">show mls netflow</a>	Displays configuration information about the NetFlow hardware.

# mls ip

To enable MLS IP for the internal router on the interface, use the **mls ip** command. To disable MLS IP on the interface, use the **no** form of this command.

**mls ip**

**no mls ip**

---

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

---

**Defaults** Multicast is disabled.

---

**Command Modes** Interface configuration

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Examples** This example shows how to enable shortcuts for MLS IP:

```
Router(config-if)# mls ip
Router(config-if)#
```

---

Related Commands	Command	Description
	<a href="#">mls rp ip (interface configuration mode)</a>	Allows the external systems to enable MLS IP on a specified interface.
	<a href="#">show mls ip multicast</a>	Displays the MLS IP information.

---

# mls ip acl port expand

To enable ACL-specific features for Layer 4, use the **mls ip acl port expand** command. To disable the ACL-specific Layer 4 features, use the **no** form of this command.

**mls ip acl port expand**

**no mls ip acl port expand**

---

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

---

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

---

**Command Modes** Global configuration

---

Release	Modification
12.2(18)ZY	Support for this command was introduced.

---

---

**Examples** This example shows how to enable the expansion of ACL logical operations on Layer 4 ports:

```
Router(config)# mls ip acl port expand
Router(config)#
```

## mls ip cef accounting per-prefix

To enable MLS per-prefix accounting, use the **mls ip cef accounting per-prefix** command. To disable MLS per-prefix accounting, use the **no** form of this command

```
mls ip cef accounting per-prefix prefix-entry prefix-entry-mask [instance-name]
```

```
no mls ip cef accounting per-prefix
```

Syntax Description		
	<i>prefix</i>	Prefix entry in the format A.B.C.D.
	<i>prefix-entry-mask</i>	Prefix entry mask in the format A.B.C.D.
	<i>instance-name</i>	(Optional) VPN routing and forwarding instance name.

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

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Per-prefix accounting collects the adjacency counters used by the prefix. When the prefix is used for accounting, the adjacency cannot be shared with other prefixes. You can use per-prefix accounting to account for the packets sent to a specific destination.

**Examples** This example shows how to enable MLS per-prefix accounting:

```
Router(config)# mls ip cef accounting per-prefix 172.20.52.18 255.255.255.255
Router(config)#
```

This example shows how to disable MLS per-prefix accounting:

```
Router(config)# no mls ip cef accounting per-prefix
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show mls cef ip accounting per-prefix</a>	Displays all the prefixes that are configured for the statistic collection.

# mls ip cef load-sharing

To configure the CEF load balancing, use the **mls ip cef load-sharing** command. To return to the default settings, use the **no** form of this command.

**mls ip cef load-sharing** [**full** [**exclude-port** {**destination** | **source**}] ] [**simple**]

**no mls ip cef load-sharing**

Syntax Description	full	(Optional) Sets the CEF load balancing to include source and destination Layer 4 ports and source and destination IP addresses (Layer 3).
	<b>exclude-port destination</b>	(Optional) Excludes the destination Layer 4 ports and source and destination IP addresses (Layer 3) from the load-balancing algorithm.
	<b>exclude-port source</b>	(Optional) Excludes the source Layer 4 ports and source and destination IP addresses (Layer 3) from the load-balancing algorithm.
	<b>simple</b>	(Optional) Sets the CEF load balancing for single-stage load sharing.

**Defaults** Source and destination IP address and universal identification

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **mls ip cef load-sharing** command affects the IPv4, the IPv6, and the MPLS forwardings. The **mls ip cef load-sharing** command is structured as follows:

- **mls ip cef load-sharing full**—Uses Layer 3 and Layer 4 information with multiple adjacencies.
- **mls ip cef load-sharing full simple**—Uses Layer 3 and Layer 4 information without multiple adjacencies.
- **mls ip cef load-sharing simple**—Uses Layer 3 information without multiple adjacencies.

For additional guidelines, refer to the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*.

**Examples** This example shows how to set load balancing to include Layer 3 and Layer 4 ports with multiple adjacencies:

```
Router(config)# mls ip cef load-sharing full
Router(config)#
```

This example shows how to set load balancing to exclude the destination Layer 4 ports and source and destination IP addresses (Layer 3) from the load-balancing algorithm:

```
Router(config)# mls ip cef load-sharing full exclude-port destination
Router(config)#
```

This example shows how to set load balancing to exclude the source Layer 4 ports and source and destination IP addresses (Layer 3) from the load-balancing algorithm:

```
Router(config)# mls ip cef load-sharing full exclude-port source
Router(config)#
```

This example shows how to return to the default setting:

```
Router(config)# no mls ip cef load-sharing
Router(config)#
```

---

**Related Commands**

Command	Description
<a href="#">show mls cef ip</a>	Displays the IP entries in the MLS-hardware Layer 3-switching table.

## mls ip cef rate-limit

To rate-limit CEF-punted data packets, use the **mls ip cef rate-limit** command. To disable the rate-limited CEF-punted data packets, use the **no** form of this command.

**mls ip cef rate-limit** *pps*

**no mls ip cef rate-limit**

Syntax	Description
<i>pps</i>	Number of data packets; valid values are from 0 to 1000000.

Defaults	Description
	No rate limit is configured.

Command Modes	Description
	Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

Certain denial-of-service attacks target the route processing engines of routers. Certain packets that cannot be forwarded by the PFC are directed to the PISA for processing. Denial-of-service attacks can overload the route processing engine and cause routing instability when running dynamic routing protocols. You can use the **mls ip cef rate-limit** command to limit the amount of traffic that is sent to the PISA to prevent denial-of-service attacks against the route processing engine.

This command rate limits all CEF-punted data packets including the following:

- Data packets going to the local interface IP address
- Data packets requiring ARP

Setting the rate to a low value could impact the packets that are destined to the IP addresses of the local interfaces and the packets that require ARP. You should use this command to limit these packets to a normal rate and to avoid abnormal incoming rates.

For additional guidelines, refer to the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*.

**Examples**

This example shows how to enable and set rate limiting:

```
Router(config)# mls ip cef rate-limit 50000
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show mls cef ip</a>	Displays the IP entries in the MLS-hardware Layer 3-switching table.

## mls ip cef rpf hw-enable-rpf-acl

To enable hardware uRPF for packets matching the deny ace when uRPF with ACL is enabled, use the **mls ip cef rpf hw-enable-rpf-acl** command. To disable hardware uRPF when RPF and ACL are enabled, use the **no** form of this command.

**mls ip cef rpf hw-enable-rpf-acl**

**no mls ip cef rpf hw-enable-rpf-acl**

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

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

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** If you do not enter the **mls ip cef rpf hw-enable-rpf-acl** command, when the uRPF with ACL is specified, packets that are permitted by the uRPF ACL are forwarded in hardware and the denied packets are sent to the PISA for the uRPF check. This command enables hardware forwarding with the uRPF check for the packets that are denied by the uRPF ACL. However in this case packets permitted by uRPF ACL are sent to the PISA for forwarding.

uRPF is not supported on PVLAN host ports.

**Examples** This example shows how to enable hardware uRPF when RPF and ACL are enabled:

```
Router(config)# mls ip cef rpf hw-enable-rpf-acl
Router(config)#
```

This example shows how to disable hardware uRPF when RPF and ACL are enabled:

```
Router(config)# no mls ip cef rpf hw-enable-rpf-acl
Router(config)#
```

Related Commands	Command	Description
	<a href="#">ip verify unicast source reachable-via {any   rx}</a>	Enables and configures RPF checks with ACL.

# mls ip cef rpf interface-group

To define an interface group in the RPF-VLAN table, use the **mls ip cef rpf interface-group** command. To delete the interface group, use the **no** form of this command.

**mls ip cef rpf interface-group** *group-number interface1 interface2 interface3* [...]

**no mls ip cef rpf interface-group** *group-number interface1 interface2 interface3* [...]

Syntax Description	
<i>group-number</i>	Interface group number; valid values are from 1 to 4.
<i>interface</i>	Interface number; see the “Usage Guidelines” section for formatting guidelines.
...	(Optional) Additional interface numbers; see the “Usage Guidelines” section for additional information.

**Defaults** No groups are configured.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** A single interface group contains three to six interfaces. You can configure up to four interface groups. For each interface group, the first four entries are installed in the hardware RPF-VLAN table.

Enter the *interface* as *interface-type**mod/port*.

Separate each interface entry with a space. You do not have to include a space between the *interface-type* and the *mod/port* arguments. See the “Examples” section for a sample entry.

**Examples** This example shows how to define an interface group:

```
Router(config)# mls ip cef rpf interface-group 0 F2/1 F2/2 F2/3 F2/4 F2/5 F2/6
Router(config)#
```

## mls ip cef rpf multipath

To configure the RPF modes, use the **mls ip cef rpf multipath** command. To return to the default settings, use the **no** form of this command.

**mls ip cef rpf multipath { interface-group | punt | pass }**

Syntax Description	interface-group	Description
	<b>interface-group</b>	Disables the RPF check for packets coming from multiple path routes; see the “Usage Guidelines” section for additional information.
	<b>punt</b>	Redirects the RPF-failed packets to the route processor for multiple path prefix support.
	<b>pass</b>	Disables the RPF check for packets coming from multiple path routes.

**Defaults** punt

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

The interface-group mode is similar to the pass mode but utilizes the RPF\_VLAN global table for the RPF check. Packets from other multiple path prefixes always pass the RPF check.

You enter the **mls ip cef rpf multipath interface-group** command to define an RPF\_VLAN table interface group. One interface group contains from three to six interfaces, and you can configure up to four interface groups. For each interface group, the first four entries are installed in the hardware RPF\_VLAN table. For the prefix that has more than three multiple paths, and all paths except two are part of that interface group, the FIB entry of that prefix uses this RPF\_VLAN entry.

### Examples

This example shows how to redirect the RPF-failed packets to the route processor for multiple path prefix support:

```
Router(config)# mls ip cef rpf multipath interface-group
Router(config)#
```

### Related Commands

Command	Description
<a href="#">show mls cef ip</a>	Displays the IP entries in the MLS-hardware Layer 3-switching table.

# mls ip delete-threshold

To delete the configured ACL thresholds, use the **mls ip delete-threshold** command.

**mls ip delete-threshold** *acl-num*

<b>Syntax Description</b>	<i>acl-num</i> Reflective ACL number; valid values are from 1 to 10000.						
<b>Defaults</b>	This command has no default settings.						
<b>Command Modes</b>	Global configuration						
<b>Command History</b>	<table border="1"> <thead> <tr> <th style="border-bottom: 1px solid black;">Release</th> <th style="border-bottom: 1px solid black;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border-bottom: 1px solid black;">12.2(18)ZY</td> <td style="border-bottom: 1px solid black;">Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)ZY	Support for this command was introduced.		
Release	Modification						
12.2(18)ZY	Support for this command was introduced.						
<b>Usage Guidelines</b>	The <b>mls ip delete-threshold</b> command is active only when you enable the <b>mls ip reflexive ndr-entry tcam</b> command.						
<b>Examples</b>	<p>This example shows how to delete an ACL threshold:</p> <pre>Router(config)# mls ip delete-threshold 223 Router(config)#</pre>						
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th style="border-bottom: 1px solid black;">Command</th> <th style="border-bottom: 1px solid black;">Description</th> </tr> </thead> <tbody> <tr> <td style="border-bottom: 1px solid black;"><b>mls ip install-threshold</b></td> <td style="border-bottom: 1px solid black;">Installs the configured ACL thresholds.</td> </tr> <tr> <td style="border-bottom: 1px solid black;"><b>mls ip reflexive ndr-entry tcam</b></td> <td style="border-bottom: 1px solid black;">Enables the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR.</td> </tr> </tbody> </table>	Command	Description	<b>mls ip install-threshold</b>	Installs the configured ACL thresholds.	<b>mls ip reflexive ndr-entry tcam</b>	Enables the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR.
Command	Description						
<b>mls ip install-threshold</b>	Installs the configured ACL thresholds.						
<b>mls ip reflexive ndr-entry tcam</b>	Enables the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR.						

## mls ip directed-broadcast

To enable the hardware switching of the IP-directed broadcasts, use the **mls ip directed-broadcast** command. To return to the default settings, use the **no** form of this command.

**mls ip directed-broadcast** { **exclude-router** | **include-router** }

**no mls ip directed-broadcast**

Syntax Description	exclude-router	include-router
	Forwards the IP-directed broadcast packet in the hardware to all hosts in the VLAN except the router.	Forwards the IP-directed broadcast packet in the hardware to all hosts in the VLAN including the router.

**Defaults** Disabled

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

The **exclude-router** and **include-router** keywords both support hardware switching, but **exclude-router** does not send a copy of the hardware-switched packets to the router. If you enter the **include-router** keyword, the router does not forward the IP-directed broadcast packet again.

In the default mode, IP-directed broadcast packets are not forwarded in the hardware; they are handled at the process level by the PISA. The PISA decision to forward or not forward the packet is dependent on the **ip directed-broadcast** command configuration.

There is no interaction between the **ip directed-broadcast** command and the **mls ip directed-broadcast** command. The **ip directed-broadcast** command involves software forwarding, and the **mls ip directed-broadcast** command involves hardware forwarding.

MLS IP-directed broadcast supports a secondary interface address.

Any packets that hit the CPU are not forwarded unless you add the **ip directed-broadcast** command to the same interface.

You can configure the MLS IP-directed broadcasts on a port-channel interface but not on the physical interfaces on the port-channel interface. If you want to add a physical interface to a port-channel group, the physical interface cannot have the MLS IP-directed broadcast configuration. You have to first remove the configuration manually and then add the physical interface to the channel group. If a physical interface is already part of a channel group, the CLI will not accept the **mls ip directed-broadcast** configuration command on that physical interface.

---

**Examples**

This example shows how to forward the IP-directed broadcast packet in the hardware to all hosts in the VLAN with the exception of the router:

```
Router(config-if)# mls ip directed-broadcast exclude-router
Router(config-if)#
```

This example shows how to forward the IP-directed broadcast packet in the hardware to all hosts in the VLAN:

```
Router(config-if)# mls ip directed-broadcast include-router
Router(config-if)#
```

---

**Related Commands**

Command	Description
<a href="#">show mls cef adjacency</a>	Displays hardware-switched IP-directed broadcast information.

---

## mls ip inspect

To permit traffic through any ACLs that would deny the traffic through other interfaces, use the **mls ip inspect** command. To return to the default settings, use the **no** form of this command.

**mls ip inspect** *acl-name*

**no mls ip inspect** *acl-name*

Syntax Description	<i>acl-name</i> ACL name.				
Defaults	Disabled				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Release</th> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border-bottom: 1px solid black;">12.2(18)ZY</td> <td style="border-bottom: 1px solid black;">Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)ZY	Support for this command was introduced.
Release	Modification				
12.2(18)ZY	Support for this command was introduced.				
Usage Guidelines	On a Catalyst 6500 series switch, when interfaces are configured to deny traffic, the CBAC permits traffic to flow bidirectionally only through the interface that is configured with the <b>ip inspect</b> command.				
Examples	<p>This example shows how to permit the traffic through a specific ACL (named deny_ftp_c):</p> <pre>Router(config)# mls ip inspect deny_ftp_c Router(config)#</pre>				
Related Commands	<table border="1"> <thead> <tr> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Command</th> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Description</th> </tr> </thead> <tbody> <tr> <td style="border-bottom: 1px solid black;"><b>ip inspect</b></td> <td style="border-bottom: 1px solid black;">Applies a set of inspection rules to an interface.</td> </tr> </tbody> </table>	Command	Description	<b>ip inspect</b>	Applies a set of inspection rules to an interface.
Command	Description				
<b>ip inspect</b>	Applies a set of inspection rules to an interface.				

# mls ip install-threshold

To install the configured ACL thresholds, use the **mls ip install-threshold** command.

**mls ip install-threshold** *acl-num*

<b>Syntax Description</b>	<i>acl-num</i> Reflective ACL number; valid values are from 1 to 10000.						
<b>Defaults</b>	This command has no default settings.						
<b>Command Modes</b>	Global configuration						
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(18)ZY</td> <td>Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)ZY	Support for this command was introduced.		
Release	Modification						
12.2(18)ZY	Support for this command was introduced.						
<b>Usage Guidelines</b>	The <b>mls ip install-threshold</b> command is active only when you enable the <b>mls ip reflexive ndr-entry team</b> command.						
<b>Examples</b>	<p>This example shows how to install an ACL threshold:</p> <pre>Router(config)# mls ip install-threshold 123 Router(config)#</pre>						
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>mls ip delete-threshold</b></td> <td>Deletes configured ACL thresholds.</td> </tr> <tr> <td><b>mls ip reflexive ndr-entry team</b></td> <td>Enables the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR.</td> </tr> </tbody> </table>	Command	Description	<b>mls ip delete-threshold</b>	Deletes configured ACL thresholds.	<b>mls ip reflexive ndr-entry team</b>	Enables the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR.
Command	Description						
<b>mls ip delete-threshold</b>	Deletes configured ACL thresholds.						
<b>mls ip reflexive ndr-entry team</b>	Enables the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR.						

## mls ip multicast (global configuration mode)

To enable MLS IP and configure the hardware switching globally, use the **mls ip multicast** command. To disable MLS IP, use the **no** form of this command.

**mls ip multicast** [**capability**]

**mls ip multicast** [**vrf** *name*] [**connected** | **egress local** | **mfd** | **refresh-state** | **shared-tree-mfd** | **threshold** *ppsec*]

**no mls ip multicast** [**vrf**]

Syntax Description	
<b>capability</b>	(Optional) Exports the information about the egress capability from the switch processor to the route processor.
<b>vrf</b> <i>name</i>	(Optional) Specifies the VRF name.
<b>connected</b>	(Optional) Installs the interface/mask entries for bridging directly connected sources to the internal router.
<b>egress local</b>	(Optional) Populates the multicast expansion table with local Layer 3-routed interfaces.
<b>mfd</b>	(Optional) Enables complete hardware switching.
<b>refresh-state</b>	(Optional) Refreshes the expiration time of the (S,G) entry or the (*,G) entry with NULL OIF.
<b>shared-tree-mfd</b>	(Optional) Enables the complete shortcut for (*,G) flows.
<b>threshold</b> <i>ppsec</i>	(Optional) Sets the minimum traffic rate; below this rate, the flow is switched in the software instead of in the hardware. Valid values are from 10 to 10000 seconds.

### Defaults

The defaults are as follows:

- Multicast is disabled.
- Hardware switching is allowed for all eligible multicast routes.
- **connected** is enabled.
- **egress local** is disabled.
- **mfd** is enabled.
- **refresh-state** is enabled.
- **shared-tree-mfd** is enabled.

### Command Modes

Global configuration

**Command History**

Release	Modification
12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines****Note**

After you enter the **mls ip multicast egress local** command, you must perform a system reset for the configuration to take effect.

When entering the **mls ip multicast egress local** command, ensure that IPv6 multicast is not enabled. Since the egress multicast replication performance enhancement feature cannot separately turn on or turn off IPv4 and IPv6, you cannot have IPv4 and IPv6 multicast enabled when this feature is turned on.

These optional keywords are supported:

- **threshold**
- **connected**
- **refresh-state**
- **shared-tree-mfd**
- **mfd**

The **threshold** *ppsec* optional keyword and argument do not impact flows that are already populated in the hardware cache.

The expiration time refresh is updated when flow statistics are received from the Catalyst 6500 series switch (indicating that the traffic is received from the RPF interface).

**Examples**

This example shows how to enable the MLS IP shortcuts:

```
Router(config)# mls ip multicast
Router(config)#
```

This example shows how to enable the hardware switching on a specific multicast route:

```
Router(config)# mls ip multicast vrf test1
Router(config)#
```

This example shows how to export the information about egress capability from the switch processor to the route processor:

```
Router(config)# mls ip multicast capability
Router(config)#
```

This example shows how to populate the multicast expansion table with local Layer 3-routed interfaces:

```
Router(config)# mls ip multicast egress local
Router(config)#
```

**Related Commands**

Command	Description
<a href="#">mls rp ip (global configuration mode)</a>	Enables external systems to establish IP shortcuts to the PISA.
<a href="#">show mls ip multicast</a>	Displays the MLS IP information.

## mls ip multicast (interface configuration mode)

To enable MLS IP shortcuts on the interface, use the **mls ip multicast** command. To disable MLS IP shortcuts on the interface, use the **no** form of this command.

**mls ip multicast**

**no mls ip multicast**

---

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

---

**Defaults** Multicast is disabled.

---

**Command Modes** Interface configuration

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Examples** This example shows how to enable the MLS IP shortcuts:

```
Router(config-if)# mls ip multicast
Router(config-if)#
```

---

Related Commands	Command	Description
	<a href="#">show mls ip multicast</a>	Displays the MLS IP information.

---

# mls ip multicast bidir gm-scan-interval

To set the RPF scan interval for the Bidir rendezvous point, use the **mls ip multicast bidir gm-scan-interval** command. To disable the RPF scan interval for the Bidir rendezvous point, use the **no** form of this command.

**mls ip multicast bidir gm-scan-interval** *interval*

**no mls ip multicast bidir gm-scan-interval**

<b>Syntax Description</b>	<i>interval</i>	RPF scan interval for the Bidir rendezvous point; valid values are from 1 to 1000 seconds.
---------------------------	-----------------	--

<b>Defaults</b>	10 seconds
-----------------	------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	When you set the RPF scan interval for the Bidir rendezvous point, you set the time that the periodic scan timer updates the RPF in the DF table for all Bidir rendezvous points in the hardware.
-------------------------	---

<b>Examples</b>	This example shows how to set the RPF scan interval for the Bidir rendezvous point:
-----------------	---

```
Router(config)# mls ip multicast bidir gm-scan-interval 30
Router(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show mls ip multicast bidir</a>	Displays the Bidir hardware-switched entries.

## mls ip multicast connected

To enable the downloading of directly connected subnets globally, use the **mls ip multicast connected** command. To disable the downloading of directly connected subnets globally, use the **no** form of this command.

**mls ip multicast connected**

**no mls ip multicast connected**

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

**Defaults** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Do not create directly connected subnets for the following cases:

- To make more room available in the FIB TCAM
- The switch is the first-hop router for a source
- The entries are for Bidir, SSM, and DM mode groups

In these cases, if you enable the downloading of directly connected subnets, the directly connected source hits the MMLS (\*,G) entry and is switched using the MMLS (\*,G) entry. The registers are not sent to the route processor (in the case of PIM-SM), and the (S,G) state is not created on the first hop (in the case of PIM-DM).

The subnet entry is installed in the TCAM entries with a shorter mask to catch directly connected sources before they hit such entries. You can punt traffic from directly connected sources to the PISA. Once the PISA sees this traffic, it can install an MMLS (S,G) entry for this source, which gets installed before the subnet entry in the TCAM. New packets from this source are now switched with the (S,G) entry.

---

**Examples**

This example shows how to enable the downloading of directly connected subnets:

```
Router(config)# mls ip multicast connected
Router(config)#
```

---

**Related Commands**

Command	Description
<a href="#">mls ip multicast (global configuration mode)</a>	Enables MLS IP and configures the hardware switching globally.
<a href="#">show mls ip multicast</a>	Displays the MLS IP information.

---

# mls ip multicast consistency-check

To enable and configure the hardware-shortcut consistency checker, use the **mls ip multicast consistency-check** command. To disable the consistency checkers, use the **no** form of this command.

```
mls ip multicast consistency-check [{settle-time seconds} | {type scan-mroute
[count count-number] | {settle-time seconds}} | {period seconds}]
```

```
no mls ip multicast consistency-check
```

## Syntax Description

<b>settle-time</b> <i>seconds</i>	(Optional) Specifies the settle time for entry/oif for the consistency checker; valid values are from 2 to 3600 seconds.
<b>type scan-mroute</b>	(Optional) Specifies the type of consistency check as a scan check of the mroute table.
<b>count</b> <i>count-number</i>	(Optional) Specifies the maximum number of prefixes to check per scan; valid values are from 2 to 500.
<b>period</b> <i>seconds</i>	(Optional) Specifies the period between scans; valid values are from 2 to 3600 seconds.

## Defaults

The defaults are as follows:

- Consistency check is enabled.
- **count** *count-number* is **20**.
- **period** *seconds* is **2** seconds.
- **settle-time** *seconds* is **60** seconds.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

The *oif* entry is the outgoing interface of a multicast {\*,G} or {source, group} flow.

The consistency checker scans the mroute table and assures that the multicast-hardware entries are consistent with the mroute table. Whenever an inconsistency is detected, the inconsistency is automatically corrected.

To display the inconsistency error, use the **show mls ip multicast consistency-check** command.

**Examples**

This example shows how to enable the hardware-shortcut consistency checker:

```
Router (config)# mls ip multicast consistency-check
Router (config)#
```

This example shows how to enable the hardware-shortcut consistency checker and configure the scan check of the mroute table:

```
Router (config)# mls ip multicast consistency-check type scan-mroute count 20 period 35
Router (config)#
```

This example shows how to enable the hardware-shortcut consistency checker and specify the period between scans:

```
Router (config)# mls ip multicast consistency-check type scan-mroute period 35
Router (config)#
```

**Related Commands**

Command	Description
<a href="#">show mls ip multicast consistency-check</a>	Displays the MLS IP information.

## mls ip multicast flow-stat-timer

To set the time interval between two consecutive batches of flow-statistics messages from the switch processor to the route processor, use the **mls ip multicast flow-stat-timer** command. To return to the default settings, use the **no** form of this command.

**mls ip multicast flow-stat-timer** *num*

**no mls ip multicast flow-stat-timer**

### Syntax Description

<i>num</i>	Time interval between two consecutive batches of flow-statistics messages from the switch processor to the route processor.
------------	---

### Defaults

25 seconds

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Examples

This example shows how to configure the time interval between two consecutive batches of flow-statistics messages from the switch processor to the route processor:

```
Router (config)# mls ip multicast flow-stat-timer 10
Router (config)#
```

### Related Commands

Command	Description
<a href="#">show mls ip multicast</a>	Displays the MLS IP information.

# mls ip multicast replication-mode

To enable and specify the replication mode, use the **mls ip multicast replication-mode** command. To restore the system to automatic detection mode, use the **no** form of this command.

**mls ip multicast replication-mode { egress | ingress }**

**no mls ip multicast replication-mode { egress | ingress }**

Syntax Description	Command	Description
	<b>egress</b>	Forces the system to the egress mode of replication.
	<b>ingress</b>	Forces the system to the ingress mode of replication.

**Defaults** ingress

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The Supervisor Engine 32 PISA does not support the **egress** keyword.



**Note**

During the change from egress- to ingress-replication mode, traffic interruptions may occur because the shortcuts are purged and reinstalled. To avoid interruptions in traffic forwarding, enter the **mls ip multicast replication-mode ingress** command.

If you enter the **no mls ip multicast replication-mode ingress** command, only the forced-ingress mode resets

**Examples** This example shows how to enable the ingress-replication mode:

```
Router (config)# mls ip multicast replication-mode ingress
Router (config)#
```

Related Commands	Command	Description
	<a href="#">show mls ip multicast capability</a>	Displays the MLS IP information.

## mls ip multicast sso

To configure the SSO parameters, use the **mls ip multicast sso** command. To return to the default settings, use the **no** form of this command.

```
mls ip multicast sso {{ convergence-time time } | { leak interval } | { leak percentage } }
```

Syntax Description	Parameter	Description
	<b>convergence-time</b> <i>time</i>	Specifies the maximum time to wait for protocol convergence; valid values are from 0 to 3600 seconds.
	<b>leak</b> <i>interval</i>	Specifies the packet-leak interval; valid values are from 0 to 3600 seconds.
	<b>leak</b> <i>percentage</i>	Specifies the percentage of multicast packets leaked to the router during switchover so that protocol convergence can take place; valid values are from 1 to 100 percent.

### Defaults

The defaults are as follows:

- **convergence-time** *time*—20 seconds
- **leak** *interval*—60 seconds
- **leak** *percentage*—10 percent

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Examples

This example shows how to set the maximum time to wait for protocol convergence:

```
Router (config)# mls ip multicast sso convergence-time 300
Router (config)#
```

This example shows how to set the packet-leak interval:

```
Router (config)# mls ip multicast sso leak 200
Router (config)#
```

This example shows how to set the packet-leak percentage:

```
Router (config)# mls ip multicast sso leak 55
Router (config)#
```

### Related Commands

Command	Description
<a href="#">show mls ip multicast sso</a>	Displays information about multicast high-availability SSO.

# mls ip multicast stub

To enable the support for non-RPF traffic drops for PIM sparse-mode stub networks, use the **mls ip multicast stub** command. To disable support for non-RPF traffic drops for PIM sparse-mode stub networks, use the **no** form of this command.

**mls ip multicast stub**

**no mls ip multicast stub**

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

**Defaults** Multicast is disabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **mls ip multicast stub** command, creates the following filters on a routed interface or a VLAN:

- Permits IP packets from all addresses that are connected to the interface to any IP destination. An address is connected to the interface if it is within the IP address prefixes configured through the **ip address *addr mask* [secondary]** command.

This filter is meant to permit unicast and multicast packets from directly connected sources.

- Permits IP multicast packets from any source address to multicast group prefixes 224.0.0.0/24 and 224.0.1.0/24.

This filter allows packets to be sent from any source address to well-known multicast addresses; 224.0.0.0/24 is used by protocols such as PIM, OSPF, EIGRP, or NTP. Addresses in 224.0.1.0/24 are used by protocols such as AutoRP (224.0.1.39, 224.0.1.40).

- Denies any other IP multicast packets.

This deny filter is meant to inhibit any multicast packets from nondirectly connected sources and is applied to the packets received on this interface or VLAN.

The permit IP multicast packets and the deny any other IP multicast packets filters are the same for all interface or VLANs to which you configure the **mls ip multicast stub** command. The permit IP packets from all addresses that are connected to the interface to any IP destination filter is different for each interface or VLAN.

---

**Examples**

This example shows how to enable the support for the non-RPF traffic drops for the PIM sparse-mode stub networks:

```
Router(config-if)# mls ip multicast stub
Router(config-if)#
```

---

**Related Commands**

Command	Description
<a href="#">show mls ip multicast</a>	Displays the MLS IP information.

# mls ip multicast threshold

To configure a threshold rate for installing hardware shortcuts, use the **mls ip multicast threshold** command. To deconfigure the threshold, use the **no** form of this command.

**mls ip multicast threshold** *ppsec*

**no mls ip multicast threshold**

<b>Syntax Description</b>	<i>ppsec</i>	Threshold in packets per seconds; valid values are from 10 to 10000 packets per second.
---------------------------	--------------	---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	<p>Use this command to prevent creation of MLS entries for short-lived multicast flows such as join requests.</p> <p>If multicast traffic drops below the configured multicast rate threshold, all multicast traffic is routed by the PISA.</p> <p>This command does not affect already installed routes. For example, if you enter this command and the shortcuts are already installed, the shortcuts are not removed if they are disqualified. To apply the threshold to existing routes, clear the route and let it reestablish.</p>
-------------------------	--

<b>Examples</b>	This example shows how to configure the IP MLS threshold to 10 packets per second:
-----------------	--

```
Router (config)# mls ip multicast threshold 10
Router (config)#
```

<b>Related Commands</b>	Command	Description
	<a href="#">mls rp ip (global configuration mode)</a>	Enables external systems to establish IP shortcuts to the PISA.
<a href="#">show mls ip multicast</a>	Displays the MLS IP information.	

## mls ip nat netflow-frag-l4-zero

To zero out the Layer 4 information in the NetFlow lookup table for fragmented packets, use the **mls ip nat netflow-frag-l4-zero** command.

**mls ip nat netflow-frag-l4-zero**

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

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

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command is supported in PFC3BXL or PFC3B mode only.

Use the **mls ip nat netflow-frag-l4-zero** command to prevent matching the first fragment to the NetFlow shortcut (normal operation) that is sent to the software. The next fragments that are sent to the software are translated based on the Layer 4 port information from the first fragment. The translation based on the Layer 4 port information from the first fragment occurs because there are no fragment bits for matching in the NetFlow key.

When there is a large feature configuration on an interface that requires a large number of ACL TCAM entries/masks that are programmed in TCAM, if the interface is configured as a NAT-inside interface, the feature configuration may not fit in the ACL TCAM and the traffic on the interface may get switched in the software.

**Examples** This example shows how to zero out the Layer 4 information in the NetFlow lookup table for fragmented packets:

```
Router (config)# mls ip nat netflow-frag-l4-zero
Router (config)#
```

# mls ip pbr

To enable the MLS support for policy-routed packets, use the **mls ip pbr** command. To disable the MLS support for policy-routed packets, use the **no** form of this command.

**mls ip pbr [null0]**

**no mls ip pbr**

<b>Syntax Description</b>	<b>null0</b> (Optional) Enables the hardware support for the interface null0 in the route maps.
---------------------------	---

<b>Defaults</b>	MLS support for policy-routed packets is disabled.
-----------------	--

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

<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(18)ZY</td> <td>Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)ZY	Support for this command was introduced.
Release	Modification				
12.2(18)ZY	Support for this command was introduced.				

## Usage Guidelines



**Note** Do not enable PBR and SLB on the same interface; PBR-based packets are not forwarded correctly.

When you enable the hardware-policy routing by entering the **mls ip pbr** command, all policy routing occurs in the hardware and is applied to all interfaces, regardless of which interface was configured for policy routing.

Use the **null0** keyword when you have routed traffic only to enable the hardware support for the **set interface null0** in the route maps.

<b>Examples</b>	This example shows how to enable the MLS support for policy-routed packets:
-----------------	---

```
Router(config)# mls ip pbr
Router(config)#
```

<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><a href="#">show tcam interface</a></td> <td>Displays information about the interface-based TCAM.</td> </tr> <tr> <td><a href="#">vlan acl</a></td> <td></td> </tr> </tbody> </table>	Command	Description	<a href="#">show tcam interface</a>	Displays information about the interface-based TCAM.	<a href="#">vlan acl</a>	
Command	Description						
<a href="#">show tcam interface</a>	Displays information about the interface-based TCAM.						
<a href="#">vlan acl</a>							

## mls ip reflexive ndr-entry tcam

To enable the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR, use the **mls ip reflexive ndr-entry tcam** command. To disable the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR, use the **no** form of this command.

**mls ip reflexive ndr-entry tcam**

**no mls ip reflexive ndr-entry tcam**

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

**Defaults** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** When you enter the **mls ip reflexive ndr-entry tcam** command, the reflexive ACL dynamic entries are installed in TCAM instead of in NetFlow.

**Examples** This example shows how to enable the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR:

```
Router(config)# mls ip reflexive ndr-entry tcam
Router(config)#
```

This example shows how to disable the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR:

```
Router(config)# no mls ip reflexive ndr-entry tcam
Router(config)#
```

Related Commands	Command	Description
	<a href="#">mls ip delete-threshold</a>	Deletes the configured ACL thresholds.
	<a href="#">mls ip install-threshold</a>	Installs the configured ACL thresholds.

# mls ipv6 acl compress address unicast

To turn on the compression of IPv6 addresses, use the **mls ipv6 acl compress address unicast** command. To turn off the compression of IPv6 addresses, use the **no** form of this command.

**mls ipv6 acl compress address unicast**

**no mls ipv6 acl compress address unicast**

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

**Defaults** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines



### Caution

Do not enable the compression mode if you have noncompressible address types in your network. A list of compressible address types and the address compression method are listed in [Table 2-15](#).

**Table 2-15 Compressible Address Types and Methods**

Address Type	Compression Method
EUI-64 based on MAC address	This address is compressed by removing 16 bits from bit locations [39:24]. No information is lost when the hardware compresses these addresses.
Embedded IPv4 address	This address is compressed by removing the upper 16 bits. No information is lost when the hardware compresses these addresses.

*Table 2-15 Compressible Address Types and Methods (continued)*

Address Type	Compression Method
Link Local	These addresses are compressed by removing the zeros in bits [95:80] and are identified using the same packet type as the embedded IPv4 address. No information is lost when the hardware compresses these addresses.
Others	<p>If the IPv6 address does not fall into any of the above categories, it is classified as other. If the IPv6 address is classified as other, the following occurs:</p> <ul style="list-style-type: none"> <li>• If the compress mode is on, the IPv6 address is compressed similarly to the EUI-64 compression method (removal of bits [39:24]) to allow for the Layer 4 port information to be used as part of the key used to look up the QoS TCAM, but Layer 3 information is lost.</li> <li>• If the global compression mode is off, the entire 128 bits of the IPv6 address are used. The Layer 4 port information cannot be included in the key to look up the QoS TCAM because of the size constraints on the IPv6 lookup key.</li> </ul>

**Examples**

This example shows how to turn on the compression of the noncompressible IPv6 addresses:

```
Router(config)# mls ipv6 acl compress address unicast
Router(config)#
```

This example shows how to turn off the compression of the noncompressible IPv6 addresses:

```
Router(config)# no mls ipv6 acl compress address unicast
Router(config)#
```

**Related Commands**

Command	Description
<a href="#">show fm ipv6 traffic-filter</a>	Displays the IPv6 information.
<a href="#">show mls netflow ipv6</a>	Displays configuration information about the NetFlow hardware.

# mls ipv6 acl source

To deny all IPv6 packets from a source-specific address, use the **mls ipv6 acl source** command. To accept all IPv6 packets from a source-specific address, use the **no** form of this command.

```
mls ipv6 acl source {loopback | multicast}
```

```
no mls ipv6 acl source {loopback | multicast}
```

Syntax Description	loopback	Description
	loopback	Denies all IPv6 packets with a source loopback address.
	multicast	Denies all IPv6 packets with a source multicast address.

Defaults	Value
Defaults	Disabled

Command Modes	Mode
Command Modes	Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to deny all IPv6 packets with a source loopback address:

```
Router(config)# mls ipv6 acl source loopback
Router(config)#
```

This example shows how to deny all IPv6 packets with a source multicast address:

```
Router(config)# no mls ipv6 acl source multicast
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show mls netflow ipv6</a>	Displays configuration information about the NetFlow hardware.

## mls mpls (recirculation)

To enable MPLS recirculation, use the **mls mpls** command. To disable MPLS recirculation, use the **no** form of this command.

**mls mpls {recir-agg | tunnel-recir}**

**no mls mpls {recir-agg | tunnel-recir}**

Syntax Description	recir-agg	tunnel-recir
	Recirculates the MPLS aggregated-label packets (new aggregated labels are impacted only).	Recirculates the tunnel-MPLS packets.

**Defaults** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** If you do not enable tunnel-MPLS recirculation, the IPv4 and IPv4-tunneled packets that need to be labeled (for example, the packets that are encapsulated with an MPLS header) will be corrupted when they are transmitted from the Catalyst 6500 series switch.

Use the [show erm statistics](#) command to display the FIB TCAM exception status for IPv4, IPv6, and MPLS protocols.

**Examples** This example shows how to enable the aggregated-label MPLS recirculation:

```
Router(config)# mls mpls recir-agg
Router(config)#
```

This example shows how to enable the tunnel-MPLS recirculation:

```
Router(config)# mls mpls tunnel-recir
Router(config)#
```

This example shows how to disable the aggregated-label MPLS recirculation:

```
Router(config)# no mls mpls recir-agg
Router(config)#
```

This example shows how to disable the tunnel-MPLS recirculation:

```
Router(config)# no mls mpls tunnel-recir
Router(config)#
```

---

**Related Commands**

Command	Description
<code>show erm statistics</code>	Displays the FIB TCAM exception status for IPv4, IPv6, and MPLS protocols.

---

# mls mpls (guaranteed bandwidth traffic engineering)

To configure the guaranteed bandwidth traffic engineering flow parameters globally, use the **mls mpls** command. To return to the default settings, use the **no** form of this command.

```
mls mpls {{gb-te-burst burst} | {gb-te-cir-ratio ratio} | {gb-te-dscp dscp-value [markdown]} |
{gb-te-enable [global-pool]}}
```

```
no mls mpls {{gb-te-burst burst} | {gb-te-cir-ratio ratio} | {gb-te-dscp dscp-value [markdown]} |
| {gb-te-enable [global-pool]}}
```

## Syntax Description

<b>gb-te-burst</b> <i>burst</i>	Specifies the burst duration for the guaranteed bandwidth traffic engineering flows; valid values are from 100 to 30000 milliseconds.
<b>gb-te-cir-ratio</b> <i>ratio</i>	Specifies the ratio for the committed information rate policing; valid values are from 1 to 100 percent.
<b>gb-te-dscp</b> <i>dscp-value</i>	Specifies the DSCP map for the guaranteed bandwidth traffic engineering flows; valid values are from 0 to 63.
<b>markdown</b>	(Optional) Marks down or drops the nonconforming flows.
<b>gb-te-enable</b>	Enables the guaranteed bandwidth traffic engineering flow policing.
<b>global-pool</b>	(Optional) Specifies using resources allocated from the global pool to the police traffic engineering flows.

## Defaults

The default settings are as follows:

- *burst* is 1000 milliseconds.
- *ratio* is 1 percent.
- *dscp-value* is 40.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

Use the **mls qos map dscp-exp** command to reset the Exp value of the MPLS packet when the out-label gets swapped.

If you do not enable tunnel-MPLS recirculation, the IPv4 and IPv4-tunneled packets that need to be labeled (for example, the packets that are encapsulated with an MPLS header) will be corrupted when they are transmitted from the Catalyst 6500 series switch.

Use the **show erm statistics** command to display the FIB TCAM exception status for IPv4, IPv6, and MPLS protocols.

**Examples**

This example shows how to specify the burst duration for the guaranteed bandwidth traffic engineering flows:

```
Router(config)# mls mpls gb-te-burst 2000
Router(config)#
```

This example shows how to specify the ratio for CIR policing:

```
Router(config)# mls mpls gb-te-ratio 30
Router(config)#
```

This example shows how to specify the DSCP map for the guaranteed bandwidth traffic engineering flows and to drop the nonconforming flows:

```
Router(config)# mls mpls gb-te-dscp 25 markdown
Router(config)#
```

This example shows how to enable the guaranteed bandwidth traffic engineering flow policing:

```
Router(config)# mls mpls gb-te-enable
Router(config)#
```

**Related Commands**

Command	Description
<a href="#">show erm statistics</a>	Displays the FIB TCAM exception status for IPv4, IPv6, and MPLS protocols.

## mls nde flow

To specify the filter options for NDE, use the **mls nde flow** command. To clear the NDE flow filter and reset the filter to the default settings, use the **no** form of this command.

```
mls nde flow {include | exclude} {{dest-port port-num} | {destination ip-addr ip-mask} |
  {protocol {tcp | udp}} | {source ip-addr ip-mask} | {src-port port-num}}
```

```
no mls nde flow {include | exclude}
```

Syntax Description		
<b>include</b>		Allows importing of all flows except the flows matching the given filter.
<b>exclude</b>		Allows exporting of all flows matching the given filter.
<b>dest-port</b> <i>port-num</i>		Specifies the destination port to filter; valid values are from 1 to 100.
<b>destination</b> <i>ip-addr ip-mask</i>		Specifies a destination IP address and mask to filter.
<b>protocol</b>		Specifies the protocol to include or exclude.
<b>tcp</b>		Includes or excludes TCP.
<b>udp</b>		Includes or excludes UDP.
<b>source</b> <i>ip-addr ip-mask</i>		Specifies a source IP address and subnet mask bit to filter.
<b>src-port</b> <i>port-num</i>		Specifies the source port to filter.

### Defaults

The defaults are as follows:

- All expired flows are imported.
- Interface export is disabled (**no mls nde interface**).

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

The **mls nde flow** command adds filtering to the NDE. The expired flows matching the specified criteria are exported. These values are stored in NVRAM and do not clear when NDE is disabled. If any option is not specified in this command, it is treated as a wildcard. The NDE filter in NVRAM does not clear when you disable NDE.

Only one filter can be active at a time. If you do not enter the **exclude** or **include** keyword, the filter is assumed to be an inclusion filter.

The include and exclude filters are stored in NVRAM and are not removed if you disable NDE.

*ip-addr maskbits* is the simplified long subnet address format. The mask bits specify the number of bits of the network masks. For example, 172.25.2.1/22 indicates a 22-bit subnet address. The *ip-addr* is a full host address, such as 193.22.253.1/22.

---

**Examples**

This example shows how to specify an interface flow filter so that only expired flows to destination port 23 are exported (assuming that the flow mask is set to ip-flow):

```
Router(config)# mls nde flow include dest-port 23
Router(config)#
```

---

**Related Commands**

Command	Description
<a href="#">show mls netflow</a>	Displays configuration information about the NetFlow hardware.

## mls nde interface

To populate the additional fields in the NDE packets, use the **mls nde interface** command. To disable the population of the additional fields, use the **no** form of this command.

**mls nde interface**

**no mls nde interface**

---

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

---

**Defaults** Enabled

---

**Command Modes** Interface configuration

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Usage Guidelines** You can configure NDE to populate the following additional fields in the NDE packets:

- Egress interface SNMP index
- Source-autonomous system number
- Destination-autonomous system number
- IP address of the next-hop router

The ingress-interface SNMP index is always populated if the flow mask is interface-full or interface-src-dst.

For detailed information, refer to the “Configuring NDE” chapter of the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*.

---

**Examples**

This example shows how to populate the additional fields in the NDE packets:

```
Router(config)# mls nde interface
Router(config)#
```

This example shows how to disable the population of the additional fields:

```
Router(config)# no mls nde interface
Router(config)#
```

---

**Related Commands**

Command	Description
<a href="#">mls netflow</a>	Enables NetFlow to gather statistics.
<a href="#">mls netflow sampling</a>	Enables the sampled NetFlow on an interface.

## mls nde sender

To enable MLS NDE export, use the **mls nde sender** command. To disable MLS NDE export, use the **no** form of this command.

**mls nde sender** [**version** *version*]

**no mls nde sender**

<b>Syntax Description</b>	<b>version</b> <i>version</i> (Optional) Specifies the NDE version; valid values are <b>5</b> and <b>7</b> .
---------------------------	--

<b>Defaults</b>	The defaults are as follows:
-----------------	------------------------------

- MLS NDE export is disabled.
- *version* is **7**.

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

<b>Command History</b>	<table border="1"> <thead> <tr> <th style="border: none;">Release</th> <th style="border: none;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border: none;">12.2(18)ZY</td> <td style="border: none;">Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)ZY	Support for this command was introduced.
Release	Modification				
12.2(18)ZY	Support for this command was introduced.				

<b>Examples</b>	This example shows how to enable MLS NDE export:
-----------------	--

```
Router(config)# mls nde sender
Router(config)#
```

This example shows how to disable MLS NDE export:

```
Router(config)# no mls nde sender
Router(config)#
```

<b>Related Commands</b>	<table border="1"> <thead> <tr> <th style="border: none;">Command</th> <th style="border: none;">Description</th> </tr> </thead> <tbody> <tr> <td style="border: none;"><a href="#">show mls nde</a></td> <td style="border: none;">Displays information about the NDE hardware-switched flow.</td> </tr> </tbody> </table>	Command	Description	<a href="#">show mls nde</a>	Displays information about the NDE hardware-switched flow.
Command	Description				
<a href="#">show mls nde</a>	Displays information about the NDE hardware-switched flow.				

# mls netflow

To enable NetFlow to gather the statistics, use the **mls netflow** command. To disable NetFlow from gathering the statistics, use the **no** form of this command.

**mls netflow**

**no mls netflow**

Syntax Description	<b>interface</b> (Optional) Specifies statistics gathering per interface.				
Defaults	Enabled				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(18)ZY</td> <td>Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)ZY	Support for this command was introduced.
Release	Modification				
12.2(18)ZY	Support for this command was introduced.				
Usage Guidelines	<p>NetFlow gathers the statistics from traffic that flows through the Catalyst 6500 series switch and stores the statistics in the NetFlow table. You can gather the statistics globally based on a protocol or optionally per interface.</p> <p>If you are not using NDE or the Cisco IOS features that use the hardware NetFlow table (micro-flow QoS, WCCP, TCP Intercept, or Reflexive ACLs), you may safely disable the use and maintenance of the hardware NetFlow table using the <b>no mls netflow</b> command in global configuration mode.</p>				
Examples	<p>This example shows how to gather the statistics:</p> <pre>Router(config)# mls netflow Router(config)#</pre> <p>This example shows how to disable NetFlow from gathering the statistics:</p> <pre>Router(config)# no mls netflow Disabling MLS netflow entry creation1 Router(config)#</pre>				
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><a href="#">show mls netflow</a></td> <td>Displays configuration information about the NetFlow hardware.</td> </tr> </tbody> </table>	Command	Description	<a href="#">show mls netflow</a>	Displays configuration information about the NetFlow hardware.
Command	Description				
<a href="#">show mls netflow</a>	Displays configuration information about the NetFlow hardware.				

## mls netflow maximum-flows

To configure the maximum flow allocation in the NetFlow table, use the **mls netflow maximum-flows** command. To return to the default settings, use the **no** form of this command.

**mls netflow maximum-flows** [*maximum-flows*]

**no mls netflow maximum-flows**

<b>Syntax Description</b>	<i>maximum-flows</i> (Optional) Maximum number of flows; valid values are <b>16, 32, 64, 80, 96,</b> and <b>128</b> . See the “Usage Guidelines” section for additional information.
---------------------------	--

<b>Defaults</b>	<b>128</b>
-----------------	------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The value that you specify for the maximum number of flows is that value times 1000. For example, if you enter 32, you specify that 32,000 is the maximum number of permitted flows.

**Examples** This example shows how to configure the maximum flow allocation in the NetFlow table:

```
Router(config)# mls netflow maximum-flows 96
Router(config)#
```

This example shows how to return to the default setting:

```
Router(config)# no mls netflow maximum-flows
Router(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show mls netflow table-contention</b>	Displays configuration information at the table contention level for the NetFlow hardware.

# mls netflow sampling

To enable the sampled NetFlow on an interface, use the **mls netflow sampling** command. To disable the sampled NetFlow, use the **no** form of this command.

**mls netflow sampling**

**no mls netflow sampling**

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

**Defaults** Disabled

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** To enable sampling, you must enter the **mls sampling** command and the **mls netflow sampling** command on the appropriate interfaces. If you do not enter the **mls netflow sampling** command, NDE will not export flows.

Depending on the current flow mask, the sampled NetFlow can be global or per interface. For Interface-Full and Interface-Src-Dest flow masks, the sampled NetFlow is enabled on a per-interface basis. For all the other flow masks, the sampled NetFlow is always global and turned on/off for all interfaces.

Enter the **mls sampling** command to enable the sampled NetFlow globally.

**Examples** This example shows how to enable the sampled NetFlow on an interface:

```
Router(config-if)# mls netflow sampling
Router(config-if)#
```

This example shows how to disable the sampled NetFlow on an interface:

```
Router(config-if)# no mls netflow sampling
Router(config-if)#
```

Related Commands	Command	Description
	<b>mls sampling</b>	Enables the sampled NetFlow and specifies the sampling method.
	<b>show mls sampling</b>	Displays information about the sampled NDE status.

# mls netflow usage notify

To monitor the NetFlow table usage on the switch processor, use the **mls netflow usage notify** command. To return to the default settings, use the **no** form of this command.

**mls netflow usage notify** {*threshold interval*}

**no mls netflow usage notify**

Syntax Description	threshold	Percentage threshold that, if exceeded, displays a warning message; valid values are from 20 to 100 percent.
	interval	Frequency that the NetFlow table usage is checked; valid values are from 120 to 1000000 seconds.

**Defaults** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

If the NetFlow table usage monitoring is enabled and the NetFlow table usage exceeds the percentage threshold, a warning message is displayed.

NetFlow gathers statistics from traffic that flows through the Catalyst 6500 series switch and stores the statistics in the NetFlow table. You can gather statistics globally based on a protocol or optionally per interface.

If you are not using NDE or the Cisco IOS features that use the hardware NetFlow table (micro-flow QoS, WCCP, TCP Intercept, or Reflexive ACLs), you may safely disable the use and maintenance of the hardware NetFlow table using the **no mls netflow** command in global configuration mode.

**Examples** This example shows how to configure the monitoring of the NetFlow table usage on the switch processor:

```
Router(config)# mls netflow usage notify 80 300
Router(config)#
```

Related Commands	Command	Description
	<b>show mls netflow usage</b>	Displays configuration information about the NetFlow hardware.

## mls qos (global configuration mode)

To enable the QoS functionality globally, use the **mls qos** command. To disable the QoS functionality globally, use the **no** form of this command.

**mls qos**

**no mls qos**

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

**Defaults** QoS is globally disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** If you enable QoS globally, QoS is enabled on all interfaces with the exception of the interfaces where you disabled QoS. If you disable QoS globally, all traffic is passed in QoS pass-through mode.

In port-queueing mode, PFC QoS (marking and policing) is disabled, and packet ToS and CoS are not changed by the PFC. All queueing on rcv and xmt is based on a QoS tag in the incoming packet, which is based on the incoming CoS.

For 802.1Q or ISL-encapsulated port links, queueing is based on the packet 802.1Q or ISL CoS.

For the router main interfaces or access ports, queueing is based on the configured per-port CoS (the default CoS is 0).

This command enables or disables TCAM QoS on all interfaces that are set in the OFF state.

## ■ mls qos (global configuration mode)

**Examples**

This example shows how to enable QoS globally:

```
Router(config)# mls qos
Router(config)#
```

This example shows how to disable QoS globally on the Catalyst 6500 series switch:

```
Router(config)# no mls qos
Router(config)#
```

**Related Commands**

Command	Description
<a href="#">mls qos (interface configuration mode)</a>	Enables the QoS functionality on an interface.
<a href="#">show mls qos</a>	Displays MLS QoS information.

## mls qos (interface configuration mode)

To enable the QoS functionality on an interface, use the **mls qos** command. To disable QoS functionality on an interface, use the **no** form of this command.

**mls qos**

**no mls qos**

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

**Defaults** Enabled

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Although the CLI allows you to configure PFC-based QoS on the WAN ports on the OC-12 ATM OSMs and on the WAN ports on the channelized OSMs, PFC-based QoS is not supported on the WAN ports on these OSMs.

If you disable QoS globally, it is also disabled on all interfaces.

This command enables or disables TCAM QoS (classification, marking, and policing) for the interface.

**Examples** This example shows how to enable QoS on an interface:

```
Router(config-if)# mls qos
Router(config-if)#
```

Related Commands	Command	Description
	<a href="#">mls qos (global configuration mode)</a>	Enables the QoS functionality globally.
	<a href="#">show mls qos</a>	Displays MLS QoS information.

## mls qos aggregate-policer

To define a named aggregate policer for use in policy maps, use the **mls qos aggregate-policer** command. This policer can be shared by different policy map classes and on different interfaces. To delete a named aggregate policer, use the **no** form of this command.

```
mls qos aggregate-policer name rate-bps
```

```
mls qos aggregate-policer name rate-bps burst-bytes maximum-burst-bytes
```

```
mls qos aggregate-policer name rate-bps [{ conform-action { drop [exceed-action action] } } |  
{ set-dscp-transmit [new-dscp] } | { set-prec-transmit [new-precedence] } | { transmit  
[exceed-action action] } | { violate-action action } }]
```

```
mls qos aggregate-policer aggregate-name rate-bps { pir peak-rate-bps [{ conform-action { drop  
[exceed-action action] } } | { set-dscp-transmit [new-dscp] } | { set-prec-transmit  
[new-precedence] } | { transmit [ exceed-action action ] } | { violate-action action } ] }
```

```
no mls qos aggregate-policer name
```

### Syntax Description

<i>name</i>	Name of the aggregate policer.
<i>rate-bps</i>	Maximum bits per second; valid values are from 32000 to 10000000000.
<i>burst-bytes</i>	Burst bytes; valid values are from 1000 to 31250000.
<i>maximum-burst-bytes</i>	Maximum burst bytes; valid values are from 1000 to 31250000 (if entered, must be set equal to normal-burst-bytes).
<b>conform-action</b>	(Optional) Specifies the action to be taken when the rate is not exceeded.
<b>drop</b>	(Optional) Drops the packet.
<b>exceed-action</b> <i>action</i>	(Optional) Specifies the action to be taken when QoS values are exceeded; see the “Usage Guidelines” section for valid values.
<b>set-dscp-transmit</b>	Sets the DSCP value and sends the packet.
<i>new-dscp</i>	(Optional) New DSCP value; valid values are from 0 to 63.
<b>set-prec-transmit</b>	Rewrites packet precedence and sends the packet.
<i>new-precedence</i>	(Optional) New precedence value; valid values are from 0 to 7.
<b>violate-action</b> <i>action</i>	(Optional) Specifies the action to be taken when QoS values are violated; see the “Usage Guidelines” section for valid values.
<b>pir</b> <i>peak-rate-bps</i>	Sets the PIR peak rate; valid values are from 32000 to 10000000000.

### Defaults

The defaults are as follows:

- *extended-burst-bytes* is equal to *burst-bytes*.
- **conform-action** is **transmit**.
- **exceed-action** is **drop**.
- **violate-action** is equal to the **exceed-action**.
- **pir** *peak-rate-bps* is equal to the normal (**cir**) rate.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Valid values for *action* are as follows:

- **drop**—Drops the packet
- **policed-dscp-transmit**—Changes the DSCP per the policed-DSCP map and sends it
- **transmit**—Transmits the package

The Catalyst 6500 series switch supports up to 1023 aggregates and 1023 policing rules.

The **mls qos aggregate-policer** command allows you to configure an aggregate flow and a policing rule for that aggregate. When you enter the rate and burst parameters, the range for the average rate is 32 Kbps to 4 Gbps (entered as 32000 and 4000000000) and the range for the burst size is 1 KB (entered as 1000) to 512 MB (entered as 512000000). Modifying an existing aggregate rate limit entry causes that entry to be modified in NVRAM and in the Catalyst 6500 series switch if that entry is currently being used.



**Note**

Due to hardware granularity, the rate value is limited so the burst that you configure may not be the value that is used.

Modifying an existing microflow or aggregate rate limit modifies that entry in NVRAM and in the Catalyst 6500 series switch if it is currently being used.

When you enter the aggregate policer name, follow these naming conventions:

- Maximum of 31 characters and may include a-z, A-Z, 0-9, the dash character (-), the underscore character (\_), and the period character (.)
- Must start with an alphabetic 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**

**Examples**

This example shows how to configure a QoS aggregate policer to allow a maximum of 100000 bits per second with a normal burst byte size of 10000, set DSCP to 48 when these rates are not exceeded, and drop packets when these rates are exceeded:

```
Router(config)# mls qos aggregate-policer micro-one 100000 10000 conform-action set-dscp
48 exceed action drop
Router(config)#
```

**Related Commands**

Command	Description
<a href="#">set ip dscp (policy-map configuration)</a>	Marks a packet by setting the IP DSCP in the ToS byte.

## mls qos bridged

To enable the microflow policing for bridged traffic on Layer 3 LAN interfaces, use the **mls qos bridged** command. To disable microflow policing for bridged traffic, use the **no** form of this command.

**mls qos bridged**

**no mls qos bridged**

---

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

---

**Defaults** Disabled

---

**Command Modes** Interface configuration

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Usage Guidelines** This command is supported on SVIs only.

---

**Examples** This example shows how to enable the microflow policing for bridged traffic on a VLAN interface:

```
Router(config-if)# mls qos bridged
Router(config-if)#
```

---

Related Commands	Command	Description
	<a href="#">show mls qos</a>	Displays MLS QoS information.

---

# mls qos channel-consistency

To enable the QoS-port attribute checks on EtherChannel bundling, use the **mls qos channel-consistency** command. To disable the QoS-port attribute checks on EtherChannel bundling, use the **no** form of this command.

**mls qos channel-consistency**

**no mls qos channel-consistency**

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

**Defaults** Enabled

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **mls qos channel-consistency** command is supported on port channels only.

**Examples** This example shows how to enable the QoS-port attribute checks on the EtherChannel bundling:

```
Router(config-if)# mls qos channel-consistency
Router(config-if)#
```

This example shows how to disable the QoS-port attribute checks on the EtherChannel bundling:

```
Router(config-if)# no mls qos channel-consistency
Router(config-if)#
```

# mls qos cos

To define the default CoS value for an interface, use the **mls qos cos** command. To remove a prior entry, use the **no** form of this command.

**mls qos cos** *cos-value*

**no mls qos cos** *cos-value*

Syntax Description	<i>cos-value</i>	Default CoS value for the interface; valid values are from 0 to 7.
--------------------	------------------	--

Defaults	The defaults are as follows: <ul style="list-style-type: none"> <li><i>cos-value</i> is <b>0</b>.</li> <li>CoS override is not configured.</li> </ul>
----------	---

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Usage Guidelines	CoS values are configurable on physical LAN ports only.
------------------	---

Examples	This example shows how to configure the default QoS CoS value as 6:
----------	---

```
Router(config-if)# mls qos cos 6
Router(config-if)#
```

Related Commands	Command	Description
	<a href="#">show mls qos</a>	Displays MLS QoS information.

# mls qos cos-mutation

To attach an ingress-CoS mutation map to the interface, use the **mls qos cos-mutation** command. To remove the ingress-CoS mutation map from the interface, use the **no** form of this command.

**mls qos cos-mutation** *cos-mutation-table-name*

**no mls qos cos-mutation**

Syntax Description	<i>cos-mutation-table-name</i>	Name of the ingress-CoS mutation table.
--------------------	--------------------------------	---

Defaults	No table is defined.
----------	----------------------

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to attach the ingress-CoS mutation map named mutemap2:

```
Router(config-if)# mls qos cos-mutation mutemap2
Router(config-if)#
```

Related Commands	Command	Description
	<a href="#">mls qos map cos-mutation</a>	Maps a packet's CoS to a new CoS value.
	<a href="#">show mls qos</a>	Displays MLS QoS information.

## mls qos dscp-mutation

To attach an egress-DSCP mutation map to the interface, use the **mls qos dscp-mutation** command. To remove the egress-DSCP mutation map from the interface, use the **no** form of this command.

**mls qos dscp-mutation** *dscp-mutation-table-name*

**no mls qos dscp-mutation**

<b>Syntax Description</b>	<i>dscp-mutation-table-name</i> Name of the egress-DSCP mutation table.
---------------------------	---

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

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Examples</b>	This example shows how to attach the egress-DSCP mutation map named mutemap1:
-----------------	---

```
Router(config-if)# mls qos dscp-mutation mutemap1
Router(config-if)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">mls qos map dscp-mutation</a>	Defines a named DSCP mutation map.
	<a href="#">show mls qos</a>	Displays MLS QoS information.

# mls qos exp-mutation

To attach an egress-EXP mutation map to the interface, use the **mls qos exp-mutation** command. To remove the egress-EXP mutation map from the interface, use the **no** form of this command.

**mls qos exp-mutation** *exp-mutation-table-name*

**no mls qos exp-mutation**

Syntax Description	<i>exp-mutation-table-name</i>	Name of the egress-EXP mutation table.
--------------------	--------------------------------	--

Defaults	No table is defined.
----------	----------------------

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Examples	This example shows how to attach the egress-exp mutation map named mutemap2:
----------	--

```
Router(config-if)# mls qos exp-mutation mutemap2
Router(config-if)#
```

Related Commands	Command	Description
	<a href="#">mls qos map dscp-mutation</a>	Defines a named DSCP mutation map.
	<a href="#">show mls qos mpls</a>	Displays an interface summary for MPLS QoS classes in the policy maps.

# mls qos loopback

To remove a router port from the SVI flood for VLANs that are carried through by the loopback cable, use the **mls qos loopback** command. To return to the default settings, use the **no** form of this command.

**mls qos loopback**

**no mls qos loopback**

---

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

---

**Defaults** Disabled

---

**Command Modes** Interface configuration

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Usage Guidelines** With **mls qos loopback** applied at the interface, the packets are not forwarded to the destination. Before you enter the **mls qos loopback** command, you must specify a MAC address for the OSM interface. The MAC address must be different from the LAN router MAC address that is used in PFC2 hardware switching.

---

**Examples** This example shows how to prevent packets from being forwarded to the destination:

```
Router (config-if)# mls qos loopback
Router (config-if)#
```

# mls qos map cos-dscp

To define the ingress CoS-to-DSCP map for trusted interfaces, use the **mls qos map cos-dscp** command. To remove a prior entry, use the **no** form of this command.

**mls qos map cos-dscp** *values*

**no mls qos map cos-dscp**

<b>Syntax Description</b>	<i>values</i>	Eight DSCP values, separated by spaces, corresponding to the CoS values; valid values are from 0 to 63.
---------------------------	---------------	---

**Defaults** The default CoS-to-DSCP configuration is listed in [Table 2-16](#).

**Table 2-16 CoS-to-DSCP Default Map**

CoS	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

**Command Modes** Global configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The CoS-to-DSCP map is used to map the CoS of packets arriving on trusted interfaces (or flows) to a DSCP where the trust type is trust-cos. This map is a table of eight CoS values (0 through 7) and their corresponding DSCP values. The Catalyst 6500 series switch has one map.

**Examples** This example shows how to configure the ingress CoS-to-DSCP map for trusted interfaces:

```
Router(config)# mls qos map cos-dscp 20 30 1 43 63 12 13 8
Router(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">mls qos map dscp-cos</a>	Defines an egress DSCP-to-CoS map.
	<a href="#">mls qos map ip-prec-dscp</a>	Defines an ingress-IP precedence-to-DSCP map for trusted interfaces.
	<a href="#">mls qos map policed-dscp</a>	Sets the mapping of policed DSCP values to marked-down DSCP values.
	<a href="#">show mls qos maps</a>	Displays information about the QoS map configuration and run-time version.

## mls qos map cos-mutation

To map a packet's CoS to a new CoS value, use the **mls qos map cos-mutation** command. To remove the map, use the **no** form of this command.

```
mls qos map cos-mutation name mutated_cos1 mutated_cos2 mutated_cos3 mutated_cos4
mutated_cos5 mutated_cos6 mutated_cos7 mutated_cos8
```

```
no mls qos map cos-mutation name
```

### Syntax Description

<i>name</i>	Name of the CoS map.
<i>mutated_cos1</i>	Eight CoS out values, separated by spaces; valid values are from 0 to 7.
...	See the "Usage Guidelines" section for additional information.
<i>mutated_cos8</i>	

### Defaults

If the CoS-to-CoS mutation map is not configured, the default CoS-to-CoS mutation mapping is listed in [Table 2-17](#).

**Table 2-17 CoS-to-CoS Default Map**

CoS-in	0	1	2	3	4	5	6	7
CoS-out	0	1	2	3	4	5	6	7

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

This command is supported on Catalyst 6500 series switches that are configured with the following modules only:

- WS-X6704-10GE
- WS-X6724-SFP
- WS-X6748-GE-TX

CoS mutation is not supported on non-802.1Q tunnel ports.

When you enter the **mls qos map cos-mutation** command, you are configuring the mutated-CoS values map to sequential ingress-CoS numbers. For example, by entering the **mls qos map cos-mutation 2 3 4 5 6 7 0 1** command, you configure this map:

CoS-in	0	1	2	3	4	5	6	7
CoS-out	2	3	4	5	6	7	0	1

Separate the eight CoS values by a space.

After you define the map in global configuration mode, you can attach the map to a port.

If QoS is disabled, the port is not in a trust CoS mode, and the port is not in 802.1Q tunneling mode. The changes appear once you put the port into trust CoS mode and the port is configured as an 802.1Q tunnel port.

Support for ingress-CoS mutation on 802.1Q tunnel ports and is on a per-port group basis only.

To avoid ingress-CoS mutation configuration failures, only create EtherChannels where all member ports support ingress-CoS mutation or where no member ports support ingress-CoS mutation. Do not create EtherChannels with mixed support for ingress-CoS mutation.

If you configure ingress-CoS mutation on a port that is a member of an EtherChannel, the ingress-CoS mutation is applied to the port-channel interface.

You can configure ingress-CoS mutation on port-channel interfaces.

### Examples

This example shows how to define a CoS-to-CoS map:

```
Router(config)# mls qos map cos-mutation test-map 5 4 3 to 1
Router(config)#
```

### Related Commands

Command	Description
<a href="#">show mls qos maps</a>	Displays information about the QoS map configuration and run-time version.

## mls qos map dscp-cos

To define an egress DSCP-to-CoS map, use the **mls qos map dscp-cos** command. To remove a prior entry, use the **no** form of this command.

**mls qos map dscp-cos** *dscp-values* **to** *cos-values*

**no mls qos map dscp-cos**

<b>Syntax Description</b>	<i>dscp-values</i>	DSCP values; valid values are from 0 to 63.
	<b>to</b>	Defines mapping.
	<i>cos-values</i>	CoS values; valid values are from 0 to 63.

**Defaults** The default DSCP-to-CoS map is listed in [Table 2-18](#).

**Table 2-18 DSCP-to-CoS Default Map**

DSCP	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
CoS	0	1	2	3	4	5	6	7

**Command Modes** Global configuration

<b>Command History</b>	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The DSCP-to-CoS map is used to map the final DSCP classification to a final CoS. This final map determines the output queue and threshold to which the packet is assigned. The CoS map is written into the ISL header or 802.1Q tag of the transmitted packet on trunk interfaces and contains a table of 64 DSCP values and the corresponding CoS values. The Catalyst 6500 series switch has one map. You can enter up to eight DSCP values separated by a space. You can enter up to eight CoS values separated by a space.

---

**Examples**

This example shows how to configure the egress DSCP-to-CoS map for trusted interfaces:

```
Router(config)# mls qos map dscp-cos 20 25 to 3
Router(config)#
```

---

**Related Commands**

Command	Description
<a href="#">mls qos map cos-dscp</a>	Defines the ingress CoS-to-DSCP map for trusted interfaces.
<a href="#">show mls qos maps</a>	Displays information about the QoS map configuration and run-time version.

# mls qos map dscp-exp

To define the final DSCP classification to the final EXP value, use the **mls qos map dscp-exp** command. To remove a prior entry, use the **no** form of this command.

**mls qos map dscp-exp** *dscp-values* **to** *exp-values*

**no mls qos map dscp-exp**

Syntax Description	
<i>dscp-values</i>	DSCP values; valid values are from 0 to 63.
<b>to</b>	Defines mapping.
<i>exp-values</i>	EXP values; valid values are from 0 to 7.

**Defaults** The default DSCP-to-EXP map is listed in [Table 2-19](#).

**Table 2-19 DSCP-to-EXP Default Map**

DSCP	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
EXP	0	1	2	3	4	5	6	7

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The DSCP-to-EXP map is used to map the final DSCP classification to a final EXP. This final map determines the output queue and threshold to which the packet is assigned. The EXP map contains a table of 64 DSCP values and the corresponding EXP values. The Catalyst 6500 series switch has one map.

You can enter up to eight DSCP values separated by a space. You can enter up to eight EXP values separated by a space.

**Examples** This example shows how to configure the final DSCP classification to a final EXP value:

```
Router(config)# mls qos map dscp-exp 20 25 to 3
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show mls qos maps</a>	Displays information about the QoS map configuration and run-time version.

# mls qos map dscp-mutation

To define a named DSCP mutation map, use the **mls qos map dscp-mutation** command. To return to the default mapping, use the **no** form of this command.

```
mls qos map dscp-mutation map-name input-dscp1 [input-dscp2 [input-dscp3 [input-dscp4
input-dscp5 [input-dscp6 [input-dscp7 [input-dscp8]]]]]]] to output-dscp
```

```
no mls qos map dscp-mutation map-name
```

Syntax Description	
<i>map-name</i>	Name of the DSCP mutation map.
<i>input-dscp#</i>	Internal DSCP value; valid values are from 0 to 63. See the “Usage Guidelines” section for additional information.
<b>to</b>	Defines mapping.
<i>output-dscp</i>	Egress DSCP value; valid values are from 0 to 63.

Defaults	
	<i>output-dscp</i> equals <i>input-dscp</i> .

Command Modes	
	Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Usage Guidelines	
	<p>When configuring a named DSCP mutation map, note the following:</p> <ul style="list-style-type: none"> <li>You can enter up to eight input DSCP values that map to a mutated DSCP value.</li> <li>You can enter multiple commands to map additional DSCP values to a mutated DSCP value.</li> <li>You can enter a separate command for each mutated DSCP value.</li> </ul> <p>You can configure 15 egress-DSCP mutation maps to mutate the internal DSCP value before it is written as the egress-DSCP value. You can attach egress-DSCP mutation maps to any interface that PFC QoS supports.</p> <p>PFC QoS derives the egress-CoS value from the internal DSCP value. If you configure egress-DSCP mutation, PFC QoS does not derive the egress-CoS value from the mutated DSCP value.</p>

---

**Examples**

This example shows how to map DSCP 30 to mutated DSCP value 8:

```
Router(config)# mls qos map dscp-mutation mutemap1 30 to 8
Router(config)#
```

---

**Related Commands**

Command	Description
<a href="#">show mls qos maps</a>	Displays information about the QoS map configuration and run-time version.

---

# mls qos map exp-dscp

To define the ingress EXP value to the internal DSCP map, use the **mls qos map exp-dscp** command. To return to the default mappings, use the **no** form of this command.

**mls qos map exp-dscp** *dscp-values*

**no mls qos map exp-dscp**

## Syntax Description

*dscp-values* Interval DSCP values; valid values are from 0 to 63.

## Defaults

The default EXP-to-DSCP map is listed in [Table 2-20](#).

**Table 2-20 EXP-to-DSCP Default Map**

EXP	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

The DSCP in these maps refers to the internal DSCP, not the packet DSCP.

The EXP-to-DSCP map is used to map the received EXP value to the internal DSCP map. This final map determines the output queue and threshold to which the packet is assigned. The EXP map contains a table of 64 DSCP values and the corresponding EXP values. The Catalyst 6500 series switch has one map.

You can enter up to eight DSCP values separated by a space.

## Examples

This example shows how to configure the received EXP value to an internal DSCP value:

```
Router(config)# mls qos map exp-dscp 20 25 30 31 32 32 33 34
Router(config)#
```

## Related Commands

Command	Description
<a href="#">mls qos map exp-mutation</a>	Maps a packet's EXP to a new EXP value.
<a href="#">show mls qos mpls</a>	Displays an interface summary for MPLS QoS classes in the policy maps.

## mls qos map exp-mutation

To map a packet's EXP to a new EXP value, use the **mls qos map exp-mutation** command. To return to the default mappings, use the **no** form of this command.

```
mls qos map exp-mutation map-name mutated-exp1 mutated-exp2 mutated-exp3 mutated-exp4
mutated-exp5 mutated-exp6 mutated-exp7 mutated-exp8
```

```
no mls qos map exp-mutation map-name
```

### Syntax Description

<i>map-name</i>	Name of the EXP-mutation map.
<i>mutated-exp#</i>	Eight EXP values, separated by spaces; valid values are from 0 to 7. See the "Usage Guidelines" section for additional information.

### Defaults

If the EXP-to-EXP mutation map is not configured, the default EXP-to-EXP mutation mapping is listed in [Table 2-21](#).

**Table 2-21 EXP-to-EXP Mutation Default Map**

EXP-in	0	1	2	3	4	5	6	7
EXP-out	0	1	2	3	4	5	6	7

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

When you enter the **mls qos map exp-mutation** command, you are configuring the mutated-EXP values map to the sequential EXP numbers. For example, by entering the **mls qos map exp-mutation 2 3 4 5 6 7 0 1** command, you configure this map:

EXP-in	0	1	2	3	4	5	6	7
EXP-out	2	3	4	5	6	7	0	1

Separate the eight EXP values by a space.

After you define the map in global configuration mode, you can attach the map to a port.

You can configure 15 ingress-EXP mutation maps to mutate the internal EXP value before it is written as the ingress-EXP value. You can attach ingress-EXP mutation maps to any interface that PFC QoS supports.

The PFC QoS derives the egress EXP value from the internal DSCP value. If you configure ingress-EXP mutation, PFC QoS does not derive the ingress-EXP value from the mutated EXP value.

---

**Examples**

This example shows how to map a packet's EXP to a new EXP value:

```
Router(config)# mls qos map exp-mutation mutemap1 1 2 3 4 5 6 7 0
Router(config)#
```

---

**Related Commands**

Command	Description
<a href="#">mls qos map exp-dscp</a>	Defines the ingress EXP value to the internal DSCP map.
<a href="#">show mls qos mpls</a>	Displays an interface summary for MPLS QoS classes in the policy maps.

## mls qos map ip-prec-dscp

To define an ingress-IP precedence-to-DSCP map for trusted interfaces, use the **mls qos map ip-prec-dscp** command. To remove a prior entry, use the **no** form of this command.

**mls qos map ip-prec-dscp** *dscp-values*

**no mls qos map ip-prec-dscp**

<b>Syntax Description</b>	<i>dscp-values</i>	DSCP values corresponding to IP precedence values 0 to 7; valid values are from 0 to 63.
---------------------------	--------------------	--

**Defaults** The default IP precedence-to-DSCP configuration is listed in [Table 2-22](#).

**Table 2-22 IP Precedence-to-DSCP Default Map**

IP-Precedence	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Use this command to map the IP precedence of IP packets arriving on trusted interfaces (or flows) to a DSCP when the trust type is trust-ipprec.

You can enter up to eight DSCP values separated by a space.

This map is a table of eight precedence values (0 through 7) and their corresponding DSCP values. The Catalyst 6500 series switch has one map. The IP precedence values are as follows:

- network **7**
- internet **6**
- critical **5**
- flash-override **4**
- flash **3**
- immediate **2**
- priority **1**
- routine **0**

**Examples**

This example shows how to configure the ingress-IP precedence-to-DSCP mapping for trusted interfaces:

```
Router(config)# mls qos map ip-prec-dscp 20 30 1 43 63 12 13 8
Router(config)#
```

**Related Commands**

Command	Description
<a href="#">mls qos map cos-dscp</a>	Defines the ingress CoS-to-DSCP map for trusted interfaces.
<a href="#">mls qos map dscp-cos</a>	Defines an egress DSCP-to-CoS map.
<a href="#">mls qos map policed-dscp</a>	Sets the mapping of policed DSCP values to marked-down DSCP values.
<a href="#">show mls qos maps</a>	Displays information about the QoS map configuration and run-time version.

## mls qos map policed-dscp

To configure the DSCP markdown map, use the **mls qos map policed-dscp** command. To remove a prior entry, use the **no** form of this command.

```
mls qos map policed-dscp { normal-burst | max-burst } dscp1 [dscp2 [dscp3 [dscp4 [dscp5 [dscp6
[dscp7 [dscp8]]]]]]] to policed-dscp
```

```
no mls qos map policed-dscp
```

### Syntax Description

<b>normal-burst</b>	Configures the markdown map used by the <b>exceed-action policed-dscp-transmit</b> keywords.
<b>max-burst</b>	Configures the markdown map used by the <b>violate-action policed-dscp-transmit</b> keywords.
<i>dscp1</i>	DSCP value; valid values are from 0 to 63.
<i>dscp2</i> through <i>dscp8</i>	(Optional) DSCP values; valid values are from 0 to 63.
<b>to</b>	Defines mapping.
<i>policed-dscp</i>	Policed-to-DSCP values; valid values are from 0 to 63.

### Defaults

No marked-down values are configured.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

The DSCP-to-policed-DSCP map determines the marked-down DSCP value that is applied to out-of-profile flows. The Catalyst 6500 series switch has one map.

You can enter up to eight DSCP values separated by a space.

You can enter up to eight policed DSCP values separated by a space.



#### Note

To avoid out-of-sequence packets, configure the DSCP-to-policed-DSCP map so that marked-down packets remain in the same queue as the in-profile traffic.

---

**Examples**

This example shows how to map multiple DSCPs to a single policed-DSCP value:

```
Router(config)# mls qos map policed-dscp normal-burst 20 25 43 to 4
Router(config)#
```

---

**Related Commands**

Command	Description
<a href="#">mls qos map cos-dscp</a>	Defines the ingress CoS-to-DSCP map for trusted interfaces.
<a href="#">mls qos map dscp-cos</a>	Defines an egress DSCP-to-CoS map.
<a href="#">mls qos map ip-prec-dscp</a>	Defines an ingress-IP precedence-to-DSCP map for trusted interfaces.
<a href="#">show mls qos</a>	Displays MLS QoS information.

## mls qos marking ignore port-trust

To mark packets even if the interface is trusted, use the **mls qos marking ignore port-trust** command. To return to the default settings, use the **no** form of this command.

**mls qos marking ignore port-trust**

**no mls qos marking ignore port-trust**

---

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

---

**Defaults** Port trust is enabled.

---

**Command Modes** Global configuration

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Usage Guidelines** Use the **mls qos marking ignore port-trust** command to mark packets even if the interface is trusted.

---

**Examples** This example shows how to mark packets even if the interface is trusted:

```
Router(config)# mls qos marking ignore port-trust
Router(config)#
```

This example shows how to enable port trust:

```
Router(config)# no mls qos marking ignore port-trust
Router(config)#
```

---

**Related Commands** [mls qos trust](#)

# mls qos marking statistics

To disable allocation of the policer-traffic class identification with set actions, use the **mls qos marking statistics** command. To return to the default settings, use the **no** form of this command.

**mls qos marking statistics**

**no mls qos marking statistics**

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

**Defaults** Enabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Use the **show policy-map interface** command to display policy-map statistics.

**Examples** This example shows how to disable the allocation of the policer-traffic class identification with set actions:

```
Router(config)# mls qos marking statistics
Router(config)#
```

This example shows how to allow the allocation of the policer-traffic class identification with set actions:

```
Router(config)# no mls qos marking statistics
Router(config)#
```

Related Commands	Command	Description
	<b>show policy-map interface</b>	Displays the statistics and the configurations of the input and output policies that are attached to an interface.

# mls qos mpls trust exp

To set the trusted state of MPLS packets only, use the **mls qos mpls trust exp** command. To set the trusted state of MPLS packets to untrusted, use the **no** form of this command.

**mls qos mpls trust exp**

**no qos mpls trust exp**

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

**Defaults** With the trusted state enabled, the defaults are as follows:

- Untrusted—The packets are marked to 0 or by policy.
- trust-cos.

With the trusted state disabled, the defaults are as follows:

- trust-exp—The port/policy trust state is ignored.
- The packets are marked by policy.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** You can enter the **mls qos mpls trust exp** command to treat MPLS packets as other Layer 2 packets for CoS and egress queuing purposes (for example, to apply port or policy trust). All trusted cases (trust CoS/IP/DSCP) are treated as trust-cos.

**Examples** This example shows how to set the trusted state of MPLS packets to trust-cos:

```
Router(config-if)# mls qos mpls trust exp
Router(config-if)#
```

This example shows how to set the trusted state of MPLS packets to untrusted:

```
Router(config-if)# no mls qos mpls trust exp
Router(config-if)#
```

Related Commands	Command	Description
	<a href="#">show mls qos mpls</a>	Displays an interface summary for MPLS QoS classes in the policy maps.

# mls qos police redirected

To turn on ACL-redirected packet policing, use the **mls qos police redirected** command. To turn off policing of ACL-redirected packets, use the **no** form of this command.

**mls qos police redirected**

**no mls qos police redirected**

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

**Defaults** Enabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Use the **no mls qos police redirected** command whenever you require NDE accuracy (if you do not require QoS-redirected packets).

**Examples** This example shows how to turn on the ACL-redirected packet policing:

```
Router(config)# mls qos police redirected
Router(config)#
```

This example shows how to turn off the ACL-redirected packet policing:

```
Router(config)# no mls qos police redirected
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show platform earl-mode</a>	Displays platform information.

# mls qos protocol

To define the routing-protocol packet policing, use the **mls qos protocol** command. To return to the default settings, use the **no** form of this command.

```
mls qos protocol protocol-name {pass-through | {police rate burst} | {precedence value
[police rate burst]}}
```

```
no mls qos protocol
```

Syntax Description	
<i>protocol-name</i>	Protocol name; valid values are <b>arp</b> , <b>bgp</b> , <b>eigrp</b> , <b>igrp</b> , <b>isis</b> , <b>ldp</b> , <b>nd</b> , <b>ospf</b> , and <b>rip</b> .
<b>pass-through</b>	Specifies pass-through mode.
<b>police rate</b>	Specifies the maximum bits per second to be policed; valid values are from 32000 to 10000000000 bits per second.
<i>burst</i>	Normal burst bytes; valid values are from 1000 to 31250000 bytes.
<b>precedence value</b>	Specifies the IP-precedence value of the protocol packets to rewrite; valid values are from 0 to 7.

## Defaults

The defaults are as follows:

- *burst* is 1000 bits per second.
- If QoS is enabled, DSCP is rewritten to zero.
- If QoS is disabled, the port is in a pass-through mode (no marking or policing is applied).

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

If you enter the **precedence value** keyword and arguments without entering the **police rate burst** keyword and arguments, only the packets from an untrusted port are marked.

You can make the protocol packets avoid the per-interface policy maps by entering the **police rate**, **pass-through**, or **precedence value** keywords and arguments.

The **mls qos protocol** command allows you to define the routing-protocol packet policing as follows:

- When you specify the **pass-through** mode, the DSCP value does not change and is not policed.
- When you set the **police rate**, the DSCP value does not change and is policed.
- When you specify the **precedence value**, the DSCP value changes for the packets that come from an untrusted port, the CoS value that is based on DSCP-to-CoS map changes, and the traffic is not policed.

- When you specify the **precedence value** and the **police rate**, the DSCP value changes, the CoS value that is based on DSCP-to-CoS map changes, and the DSCP value is policed. In this case, the DSCP value changes are based on the trust state of the port; the DSCP value is changed only for the packets that come from an untrusted port.
- If you do not enter a **precedence value**, the DSCP value is based on whether or not you have enabled MLS QoS as follows:
  - If you enabled MLS QoS and the port is untrusted, the internal DSCP value is overwritten to zero.
  - If you enabled MLS QoS and the port is trusted, then the incoming DSCP value is maintained.

You can make the protocol packets avoid policing completely if you choose the pass-through mode. If the police mode is chosen, the CIR specified is the rate that is used to police all the specified protocol's packets, both entering or leaving the Catalyst 6500 series switch.

To protect the system by ARP broadcast, you can enter the **mls qos protocol arp police bps** command.

### Examples

This example shows how to define the routing-protocol packet policing:

```
Router(config)# mls qos protocol arp police 43000
Router(config)#
```

This example shows how to avoid policing completely:

```
Router(config)# mls qos protocol arp pass-through 43000
Router(config)#
```

This example shows how to define the IP-precedence value of the protocol packets to rewrite:

```
Router(config)# mls qos protocol bgp precedence 4
Router(config)#
```

This example shows how to define the IP-precedence value of the protocol packets to rewrite and police the DSCP value:

```
Router(config)# mls qos protocol bgp precedence 4 police 32000
Router(config)#
```

### Related Commands

Command	Description
<a href="#">show mls qos protocol</a>	Displays the protocol pass-through information.

# mls qos queueing-only

To enable port-queueing mode, use the **mls qos queueing-only** command. To disable the port-queueing mode, use the **no** form of this command.

**mls qos queueing-only**

**no mls qos queueing-only**

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

**Defaults** QoS is globally disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** In port-queueing mode, PFC QoS (marking and policing) is disabled, and packet ToS and CoS are not changed by the PFC. All queueing on rcv and xmt is based on a QoS tag in the incoming packet, which is based on the incoming CoS.

For 802.1Q or ISL-encapsulated port links, queueing is based on the packet 802.1Q or ISL CoS.

For router main interfaces or access ports, queueing is based on the configured per-port CoS (the default CoS is 0).

**Examples** This example shows how to enable the port-queueing mode globally:

```
Router(config)# mls qos queueing-only
Router(config)#
```

This example shows how to disable the port-queueing mode globally:

```
Router(config)# no mls qos queueing-only
Router(config)#
```

Related Commands	Command	Description
	<a href="#">mls qos (global configuration mode)</a>	Enables the QoS functionality globally.
	<a href="#">show mls qos</a>	Displays MLS QoS information.

# mls qos queue-mode mode-dscp

To set the queueing mode to DSCP on an interface, use the **mls qos queue-mode mode-dscp** command. To return to the default settings, use the **no** form of this command.

**mls qos queue-mode mode-dscp**

**no mls qos queue-mode mode-dscp**

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

**Defaults** CoS mode.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command is supported on 10-Gigabit Ethernet ports only.

You should configure ports to trust DSCP only if they receive traffic that carries valid Layer 3 DSCP.

You can enable DSCP-based ingress queues and thresholds on WS-X6708-10GE ports to provide congestion avoidance.

For traffic from trust DSCP ports, PFC QoS uses the received DSCP value as the initial internal DSCP value. PFC QoS does not mark any traffic on ingress ports configured to trust received DSCP.

**Examples** This example shows how to set the queueing mode to DSCP on an interface:

```
Router(config-if)# mls qos queue-mode mode-dscp
Router(config-if)#
```

Related Commands	Command	Description
	<a href="#">priority-queue</a> <a href="#">queue-limit</a>	Allocates the available buffer space to a queue.
	<a href="#">show mls qos</a>	Displays MLS QoS information.

# mls qos rewrite ip dscp

To enable ToS-to-DSCP rewrite, use the **mls qos rewrite ip dscp** command. To disable ToS-to-DSCP rewrite, use the **no** form of this command.

**mls qos rewrite ip dscp**

**no mls qos rewrite ip dscp**

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

**Defaults** QoS is globally disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** If you disable ToS-to-DSCP rewrite, and QoS is enabled globally, the following occurs:

- Final ToS-to-DSCP rewrite is disabled, and the ToS-to-DSCP packet is preserved.
- Policing and marking function according to the QoS configuration.
- Marked and marked-down CoS is used for queueing.
- In QoS disabled mode, both ToS and CoS are preserved.

The **no mls qos rewrite ip dscp** command is incompatible with MPLS. The default **mls qos rewrite ip dscp** command must remain enabled in order for the PFC3BXL or PFC3B to assign the correct EXP value for the labels that it imposes.

**Examples** This example shows how to disable ToS-to-DSCP rewrite:

```
Router(config)# mls qos rewrite ip dscp
Router(config)#
```

This example shows how to disable port-queueing mode globally:

```
Router(config)# no mls qos rewrite ip dscp
Router(config)#
```

Related Commands	Command	Description
	<b>mls qos (global configuration mode)</b>	Enables the QoS functionality globally.
	<b>show mls qos</b>	Displays MLS QoS information.

## mls qos statistics-export (global configuration mode)

To enable QoS-statistics data export globally, use the **mls qos statistics-export** command. To disable QoS-statistics data export globally, use the **no** form of this command.

**mls qos statistics-export**

**no mls qos statistics-export**

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

**Defaults** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** You must enable data export globally to set up data export on your Catalyst 6500 series switch. QoS-statistics data export is not supported on OSM interfaces. For QoS-statistics data export to perform correctly, you should set the export-destination hostname or IP address and the UDP port number.

**Examples** This example shows how to enable data export globally:

```
Router(config)# mls qos statistics-export
Router(config)#
```

This example shows how to disable data export globally:

```
Router(config)# no mls qos statistics-export
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show mls qos statistics-export info</a>	Displays information about the MLS-statistics data-export status and configuration.

## mls qos statistics-export (interface configuration mode)

To enable per-port QoS-statistics data export, use the **mls qos statistics-export** command. To disable per-port QoS-statistics data export, use the **no** form of this command.

**mls qos statistics-export**

**no mls qos statistics-export**

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

**Defaults** Disabled

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** QoS-statistics data export is not supported on OSM interfaces.

You must enable data export on the port and globally to set up data export on your Catalyst 6500 series switch.

For QoS-statistics data export to perform correctly, you should set the export-destination hostname or IP address and the UDP port number.

QoS-statistics data is exported using delimiter-separated fields. You can set the delimiter by entering the **mls qos statistics-export delimiter** command.

Port statistics are exported; port QoS statistics are not exported. For each data export-enabled port, the following information is exported:

- Type (1 denotes the type of port)
- Module/port
- In packets (cumulated hardware-counter values)
- In bytes (cumulated hardware-counter values)
- Out packets (cumulated hardware-counter values)
- Out bytes (cumulated hardware-counter values)
- Time stamp (time in seconds since January 1, 1970 UTC relative)

For example, if you have QoS-statistics data export that is enabled on FastEthernet4/5, the exported records could be (in this example, the delimiter is a | [pipe]) as follows:

```
i4;4/5;453;80;45500;6800;985364894;
```

## ■ mls qos statistics-export (interface configuration mode)

**Examples**

This example shows how to enable QoS-statistics data export:

```
Router(config-if)# mls qos statistics-export
Router(config-if)#
```

This example shows how to disable QoS-statistics data export:

```
Router(config-if)# no mls qos statistics-export
Router(config-if)#
```

**Related Commands**

Command	Description
<b>mls qos statistics-export delimiter</b>	Sets the QoS-statistics data-export field delimiter.
<b>show mls qos statistics-export info</b>	Displays information about the MLS-statistics data-export status and configuration.

# mls qos statistics-export aggregate-policer

To enable QoS-statistics data export on the named aggregate policer, use the **mls qos statistics-export aggregate-policer** command. To disable QoS-statistics data export on the named aggregate policer, use the **no** form of this command.

**mls qos statistics-export aggregate-policer** *policer-name*

**no mls qos statistics-export aggregate-policer** *policer-name*

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

Defaults	Disabled for all shared aggregate policers
----------	--

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Usage Guidelines	<p>QoS-statistics data export is not supported on OSM interfaces.</p> <p>You must enable data export on the shared aggregate policer and globally to set up data export on your Catalyst 6500 series switch.</p> <p>QoS-statistics data is exported using delimiter-separated fields. You can set the delimiter by entering the <b>mls qos statistics-export delimiter</b> command.</p> <p>For each data export-enabled shared aggregate or named policer, statistics data per policer per EARL is exported. For each data export-enabled shared aggregate or named policer, the following information is exported:</p> <ul style="list-style-type: none"> <li>• Type (3 denotes aggregate policer export type)</li> <li>• Aggregate name</li> <li>• Direction (in or out)</li> <li>• EARL identification</li> <li>• Accepted packets (cumulated hardware-counter values)</li> <li>• Exceeded normal-rate packets (cumulated hardware-counter values)</li> <li>• Exceeded excess-rate packets (cumulated hardware-counter values)</li> <li>• Time stamp (time in seconds since January 1, 1970 UTC relative)</li> </ul> <p>If a shared aggregate policer is attached to policies in both directions, two records are exported (one in each direction). Each record will contain the same counter values for accepted packets, exceeded normal packet rates, and exceeded excess packet rates.</p> <p>For example, the exported records could be as follows (in this example, the delimiter is a   [pipe]):</p>
------------------	--

## ■ mls qos statistics-export aggregate-policer

```

;3;agg_4;in;4;45543;5345;985364894;
;3;agg_4;in;3;45543;5345;985364894;

```

This example indicates the following information:

- QoS-statistics data export that is enabled on the shared aggregate policer named “aggr\_1”
- An EARL in the supervisor engine that is installed in slot 1
- An EARL that is installed in slot 3

---

**Examples**

This example shows how to enable per-shared aggregate or named-policer data export:

```

Router(config)# mls qos statistics-export aggregate-policer aggr1M
Router(config)#

```

---

**Related Commands**

Command	Description
<b>mls qos statistics-export delimiter</b>	Sets the QoS-statistics data-export field delimiter.
<b>show mls qos statistics-export info</b>	Displays information about the MLS-statistics data-export status and configuration.

## mls qos statistics-export class-map

To enable QoS-statistics data export for a class map, use the **mls qos statistics-export class-map** command. To disable QoS-statistics data export for a class map, use the **no** form of this command.

**mls qos statistics-export class-map** *classmap-name*

**no mls qos statistics-export class-map** *classmap-name*

<b>Syntax Description</b>	<i>classmap-name</i> Name of the class map.				
<b>Defaults</b>	Disabled				
<b>Command Modes</b>	Global configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(18)ZY</td> <td>Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)ZY	Support for this command was introduced.
Release	Modification				
12.2(18)ZY	Support for this command was introduced.				

<b>Usage Guidelines</b>	<p>QoS-statistics data export is not supported on OSM interfaces.</p> <p>You must enable data export on the class map and globally to set up data export on your Catalyst 6500 series switch.</p> <p>QoS-statistics data is exported using delimiter-separated fields. You can set the delimiter by entering the <b>mls qos statistics-export delimiter</b> command.</p> <p>For each data export-enabled class map, the statistics data per policer per interface is exported. If the interface is a physical interface, the following information is exported:</p> <ul style="list-style-type: none"> <li>• Type (4 denotes a class map physical export)</li> <li>• Class map name</li> <li>• Direction (in or out)</li> <li>• Module/port</li> <li>• Accepted packets (cumulated hardware-counter values)</li> <li>• Exceeded normal-rate packets (cumulated hardware-counter values)</li> <li>• Exceeded excess-rate packets (cumulated hardware-ounter values)</li> <li>• Time stamp (time in seconds since January 1, 1970 UTC relative)</li> </ul> <p>If the interface is a Catalyst 6500 series switch VLAN, the following information is exported:</p> <ul style="list-style-type: none"> <li>• Type (5 denotes class-map VLAN export)</li> <li>• Class-map name</li> <li>• Direction (in or out)</li> <li>• EARL identification (slot number in which the EARL is installed)</li> </ul>
-------------------------	--

- VLAN number
- Accepted packets (cumulated hardware-counter values)
- Exceeded normal-rate packets (cumulated hardware-counter values)
- Exceeded excess-rate packets (cumulated hardware-counter values)
- Time stamp (time in seconds since January 1, 1970 UTC relative)

If the interface is a Catalyst 6500 series switch port channel, the following information is exported:

- Type (6 denotes class-map port-channel export)
- Class-map name
- Direction (in or out)
- EARL identification (slot number in which the EARL is installed)
- Port-channel number
- Accepted packets (cumulated hardware-counter values)
- Exceeded normal-rate packets (cumulated hardware-counter values)
- Exceeded excess-rate packets (cumulated hardware-counter values)
- Time stamp (time in seconds since January 1, 1970 UTC relative)

For example, if you have the following configuration:

- QoS-statistics data export enabled on the class map named “class\_1”
- An EARL in the supervisor engine that is installed in slot 1
- An EARL that is installed in slot 3
- The Catalyst 6500 series switch is in the policy map named “policy\_1”
- policy\_1 is attached to the following interfaces in the ingress direction:
  - FastEthernet4/5
  - VLAN 100
  - Port-channel 24

The exported records could be (in this example, the delimiter is a | [pipe]) as follows:

```

;4;class_4;in;4/5;45543;5345;5345;985364894;
;5;class_4;in;4;400;44000;3554;36678;985364894;
;5;class_4;in;3;400;30534;4575;4575;985364894;

```

## Examples

This example shows how to enable QoS-statistics data export for a class map:

```

Router(config)# mls qos statistics-export class-map class3
Router(config)#

```

## Related Commands

Command	Description
<a href="#">mls qos statistics-export delimiter</a>	Sets the QoS-statistics data-export field delimiter.
<a href="#">show mls qos statistics-export info</a>	Displays information about the MLS-statistics data-export status and configuration.

# mls qos statistics-export delimiter

To set the QoS-statistics data-export field delimiter, use the **mls qos statistics-export delimiter** command. To return to the default settings, use the **no** form of this command.

**mls qos statistics-export delimiter**

**no mls qos statistics-export delimiter**

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

**Defaults** The default delimiter is the pipe character (|).

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** QoS-statistics data export is not supported on OSM interfaces.  
You must enable data export globally to set up data export on your Catalyst 6500 series switch.

**Examples** This example shows how to set the QoS-statistics data-export field delimiter (a comma) and verify the configuration:

```
Router(config)# mls qos statistics-export delimiter ,
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show mls qos statistics-export info</a>	Displays information about the MLS-statistics data-export status and configuration.

## mls qos statistics-export destination

To configure the QoS-statistics data-export destination host and UDP port number, use the **mls qos statistics-export destination** command. To return to the default settings, use the **no** form of this command.

```
mls qos statistics-export destination {host-name | host-ip-address} {{port port-number} | syslog}
[facility facility-name] [severity severity-value]
```

### Syntax Description

<i>host-name</i>	Hostname.
<i>host-ip-address</i>	Host IP address.
<b>port</b> <i>port-number</i>	Specifies the UDP port number.
<b>syslog</b>	Specifies the syslog port.
<b>facility</b> <i>facility-name</i>	(Optional) Specifies the type of facility to export; see the “Usage Guidelines” section for a list of valid values.
<b>severity</b> <i>severity-value</i>	(Optional) Specifies the severity level to export; see the “Usage Guidelines” section for a list of valid values.

### Defaults

The default is none unless **syslog** is specified. If **syslog** is specified, the defaults are as follows:

- *port* is **514**.
- *facility* is **local6**.
- *severity* is **debug**.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

QoS-statistics data export is not supported on OSM interfaces.

Valid *facility* values are as follows:

- **authorization**—Security/authorization messages
- **cron**—Clock daemon
- **daemon**—System daemon
- **kernel**—Kernel messages
- **local0**—Local use 0
- **local1**—Local use 1
- **local2**—Local use 2

- **local3**—Local use 3
- **local4**—Local use 4
- **local5**—Local use 5
- **local6**—Local use 6
- **local7**—Local use 7
- **lpr**—Line printer subsystem
- **mail**—Mail system
- **news**—Network news subsystem
- **syslog**—Messages that are generated internally by syslogd
- **user**—User-level messages
- **uucp**—UUCP subsystem

Valid *severity* levels are as follows:

- **alert**—Action must be taken immediately
- **critical**—Critical conditions
- **debug**—Debug-level messages
- **emergency**—System is unusable
- **error**—Error conditions
- **informational**—Informational
- **notice**—Normal but significant conditions
- **warning**—Warning conditions

### Examples

This example shows how to specify the destination host address and syslog as the UDP port number:

```
Router(config)# mls qos statistics-export destination 172.20.52.3 syslog
Router(config)#
```

### Related Commands

Command	Description
<a href="#">show mls qos statistics-export info</a>	Displays information about the MLS-statistics data-export status and configuration.

## mls qos statistics-export interval

To specify how often a port and/or aggregate-policer QoS-statistics data is read and exported, use the **mls qos statistics-export interval** command. To return to the default settings, use the **no** form of this command.

**mls qos statistics-export interval** *interval*

**no mls qos statistics-export interval**

<b>Syntax Description</b>	<i>interval</i>	Export time; valid values are from 30 to 65535 seconds.
---------------------------	-----------------	---

<b>Defaults</b>	300 seconds
-----------------	-------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	QoS-statistics data export is not supported on OSM interfaces. The <i>interval</i> needs to be short enough to avoid counter wraparound with the activity in your configuration.
-------------------------	---



### Caution

Be careful when decreasing the interval because exporting QoS statistics increases the traffic on the Catalyst 6500 series switch.

<b>Examples</b>	This example shows how to set the QoS-statistics data-export interval:
-----------------	--

```
Router(config)# mls qos statistics-export interval 250
Router(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show mls qos statistics-export info</a>	Displays information about the MLS-statistics data-export status and configuration.

## mls qos trust

To set the trusted state of an interface, use the **mls qos trust** command. To set an interface to the untrusted state, use the **no** form of this command.

**mls qos trust [cos / dscp | ip-precedence]**

**no mls qos trust**

Syntax Description	
<b>cos</b>	(Optional) Specifies that the CoS bits in incoming frames are trusted and derives the internal DSCP value from the CoS bits.
<b>dscp</b>	(Optional) Specifies that the ToS bits in the incoming packets contain a DSCP value.
<b>ip-precedence</b>	(Optional) Specifies that the ToS bits in the incoming packets contain an IP precedence value and derives the internal DSCP value from the IP-precedence bits.

### Defaults

The defaults for LAN interfaces and WAN interfaces on the OSMs are as follows:

- If you enable global QoS, the port is untrusted.
- If you disable global QoS, the default is **dscp**.
- If you do not enter an argument, **trust dscp** is assumed.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

You can enter the **mls qos trust** command to set the trusted state of an interface. For example, you can set whether the packets arriving at an interface are trusted to carry the correct CoS, ToS, and DSCP classifications.

The **cos** keyword is not supported for **pos** or **atm** interface types.

You cannot configure the trust state on FlexWAN modules.

You cannot configure the trust state on 1q4t LAN ports except for Gigabit Ethernet ports.

Ingress-queue drop thresholds are not implemented when you enter the **mls qos trust cos** command on 4-port Gigabit Ethernet WAN modules.

Use the **set qos-group** command to set the trust state on Layer 2 WAN interfaces.

**Examples**

This example shows how to set the trusted state of an interface to IP precedence:

```
Router(config-if)# mls qos trust ip-precedence
Router(config-if)#
```

**Related Commands**

Command	Description
<a href="#">mls qos bridged</a>	Enables the microflow policing for bridged traffic on Layer 3 LAN interfaces.
<a href="#">mls qos cos</a>	Defines the default CoS value for an interface.
<a href="#">mls qos vlan-based</a>	Defines the default CoS value for a VLAN.
<a href="#">show queueing interface</a>	Displays queueing information.

# mls qos trust extend

To configure the trust mode of the phone, use the **mls qos trust extend** command. To return to the default settings, use the **no** form of this command.

**mls qos trust extend** [*cos value*]

**no mls qos trust extend**

Syntax Description	<i>cos value</i>	(Optional) Specifies the CoS value that is used to remark the packets from the PC; valid values are from 0 to 7.
--------------------	------------------	--

**Defaults** The default settings are as follows:

- Mode is untrusted.
- **cos value** is 0.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command is not supported on WAN modules.

If you set the phone to trusted mode, all the packets from the PC are sent untouched directly through the phone to the Catalyst 6500 series switch. If you set the phone to untrusted mode, all the traffic coming from the PC are remarked with the configured CoS value before being sent to the Catalyst 6500 series switch.

Each time that you enter the **mls qos trust extend** command, the mode is changed. For example, if the mode was previously set to trusted, if you enter the command, the mode changes to untrusted. Enter the **show queueing interface** command to display the current trust mode.

**Examples** This example shows how to set the phone that is attached to the switch port in trust mode:

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# mls qos trust extend
Router(config-if)#
```

This example shows how to change the mode to untrusted and set the remark CoS value to 3:

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# mls qos trust extend cos 3
Router(config-if)#
```

This example shows how to set the configuration to the default mode:

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# no mls qos trust extend
Router(config-if)#
```

---

**Related Commands**

Command	Description
<a href="#">show queueing interface</a>	Displays queueing information.

---

# mls qos vlan-based

To enable per-VLAN QoS for a Layer 2 interface, use the **mls qos vlan-based** command. To disable per-VLAN QoS for a Layer 2 interface, use the **no** form of this command.

**mls qos vlan-based**

**no mls qos vlan-based**

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

**Defaults** Disabled

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command is supported on switch-port and port-channel interfaces only.

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.

You can configure per-VLAN QoS only on Layer 2 interfaces.



**Note** 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:

```
Router(config-if)# mls qos vlan-based
Router(config-if)#
```

Related Commands	Command	Description
	<a href="#">mls qos bridged</a>	Enables the microflow policing for bridged traffic on Layer 3 LAN interfaces.
	<a href="#">mls qos cos</a>	Defines the default CoS value for an interface.
	<a href="#">show queueing interface</a>	Displays queueing information.

## mls rate-limit all

To enable and set the rate limiters common to unicast and multicast packets, use the **mls rate-limit all** command. To disable the rate limiters, use the **no** form of this command.

```
mls rate-limit all { mtu-failure | ttl-failure } pps [packets-in-burst]
```

```
no mls rate-limit all { mtu-failure | ttl-failure }
```

Syntax Description	all	Specifies rate limiting for unicast and multicast packets.
	<b>mtu-failure</b>	Enables and sets the rate limiters for MTU-failed packets.
	<b>ttl-failure</b>	Enables and sets the rate limiters for TTL-failed packets.
	<i>pps</i>	Packets per second; valid values are from 10 to 1000000 packets per second.
	<i>packets-in-burst</i>	(Optional) Packets in burst; valid values are from 1 to 255.

**Defaults** The Layer 2 rate limiters are off by default. If you enable and set the rate limiters, the default *packets-in-burst* is **10**.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Rate limiters can rate limit packets that are punted from the data path in the hardware up to the data path in the software. Rate limiters protect the control path in the software from congestion by dropping the traffic that exceeds the configured rate.

**Examples** This example shows how to set the TTL-failure limiter for unicast and multicast packets:

```
Router(config)# mls rate-limit all ttl-failure 15
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show mls rate-limit</a>	Displays information about the MLS rate limiter.

## mls rate-limit layer2

To enable and rate limit the control packets in Layer 2, use the **mls rate-limit layer2** command. To disable the rate limiter in the hardware, use the **no** form of this command.

```
mls rate-limit layer2 {pdu | l2pt | port-security} pps [packets-in-burst]
```

```
no mls rate-limit layer2 [pdu | l2pt | port-security]
```

Syntax Description		
<b>pdu</b> <i>pps</i>		Specifies the rate limit for BPDU, CDP, PDU, and VTP PDU Layer 2 control packets; valid values are from 10 to 1000000 packets per second.
<b>l2pt</b> <i>pps</i>		Specifies the rate limit for control packets in Layer 2 with a protocol-tunneling multicast-MAC address in Layer 2; valid values are from 10 to 1000000 packets per second.
<b>port-security</b> <i>pps</i>		Specifies the rate limit for port security traffic; valid values are from 10 to 1000000 packets per second.
<i>packets-in-burst</i>	(Optional)	Packets in burst; valid values are from 1 to 255.

### Defaults

The default settings are as follows:

- Layer 2 rate limiters are off by default.
- If you enable and set the rate limiters, the default setting for *packets-in-burst* is **10** and *pps* has no default setting.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

You cannot configure the Layer 2 rate limiters if the global switching mode is set to truncated mode.

For the **port-security** *pps* keywords and argument, use the following guidelines:

- The PFC2 does not support the port-security rate limiter.
- The truncated switching mode does not support the port-security rate limiter.
- The lower the value, the more the CPU is protected.

Rate limiters control packets as follows:

- The frames are classified as Layer 2 control frames by the destination MAC address. The destination MAC address used are as follows:
  - 0180.C200.0000 for IEEE BPDU
  - 0100.0CCC.CCCC for CDP
  - 0100.0CCC.CCCD for PVST/SSTP BPDU

- The software allocates an LTL index for the frames.
- The LTL index is submitted to the forwarding engine for aggregate rate limiting of all the associated frames.

The Layer 5 control packets are as follows:

- GVRP
- BPDU
- CDP/DTP/PAgP/UDLD/LACP/VTP PDUs
- PVST/SSTP PDUs

If the rate of the traffic exceeds the configured *rate*, the excessive packets are dropped at the hardware.

The **pdu** and **l2pt** rate limiters use specific hardware rate-limiter numbers only, such as 9 through 12. Enter the **show mls rate-limit usage** command to display the available rate-limiter numbers. The available numbers are displayed as “Free” in the output field. If all four rate limiters are in use by other features, a system message is displayed telling you to turn off a feature to rate limit the control packets in Layer 2.

When a MAC move occurs and a packet is seen on two ports, the packet is redirected to the software. If one of those ports has the violation mode set to restrict or protect, the packet is dropped in software. You can use the port-security rate limiter to throttle the amount of such packets redirected to software. This helps in protecting the software from high traffic rates.

## Examples

This example shows how to enable and set the rate limiters for the protocol-tunneling packets in Layer 2:

```
Router(config)# mls rate-limit layer2 l2pt 3000
Router(config)#
```

This example shows how to configure the port-security rate limiter:

```
Router(config)# mls rate-limit layer2 port-security 500
Router(config)# end
```

## Related Commands

Command	Description
<b>show mls rate-limit</b>	Displays information about the MLS rate limiter.

## mls rate-limit multicast ipv4

To enable and set the rate limiters for the IPv4 multicast packets, use the **mls rate-limit multicast ipv4** command. To disable the rate limiters, use the **no** form of this command.

```
mls rate-limit multicast ipv4 { connected | fib-miss | igmp | ip-option | partial | non-rpf } pps
[packets-in-burst]
```

```
no mls rate-limit multicast ipv4 { connected | fib-miss | igmp | ip-option | partial | non-rpf }
```

### Syntax Description

<b>connected</b>	Enables and sets the rate limiters for multicast packets from directly connected sources.
<b>fib-miss</b>	Enables and sets the rate limiters for the FIB-missed multicast packets.
<b>igmp</b>	Enables and sets the rate limiters for the IGMP packets.
<b>ip-option</b>	Enables and sets the rate limiters for the multicast packets with IP options.
<b>partial</b>	Enables and sets the rate limiters for the multicast packets during a partial SC state.
<b>non-rpf</b>	Enables and sets the rate limiters for the multicast packets failing the RPF check.
<i>pps</i>	Packets per second; valid values are from 10 to 1000000 packets per second.
<i>packets-in-burst</i>	(Optional) Packets in burst; valid values are from 1 to 255.

### Defaults

The defaults are as follows:

- If the *packets-in-burst* is not set, a default of **100** is programmed for multicast cases.
- **fib-miss**—Enabled at **100000 pps** and *packet-in-burst* is set to **100**.
- **ip-option**—Disabled.
- **partial**—Enabled at **100000 pps** and *packet-in-burst* is set to **100**.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

You cannot configure the IPv4 rate limiters if the global switching mode is set to truncated mode.

The rate limiters can rate limit the packets that are punted from the data path in the hardware up to the data path in the software. The rate limiters protect the control path in the software from congestion and drop the traffic that exceeds the configured rate.

The **ip-option** keyword is supported in PFC3BXL or PFC3B mode only.

**Examples**

This example shows how to set the rate limiters for the multicast packets failing the RPF check:

```
Router(config)# mls rate-limit multicast ipv4 non-rpf 100
Router(config)#
```

This example shows how to set the rate limiters for the multicast packets during a partial SC state:

```
Router(config)# mls rate-limit multicast ipv4 partial 250
Router(config)#
```

This example shows how to set the rate limiters for the FIB-missed multicast packets:

```
Router(config)# mls rate-limit multicast ipv4 fib-miss 15
Router(config)#
```

**Related Commands**

Command	Description
<a href="#">show mls rate-limit</a>	Displays information about the MLS rate limiter.

## mls rate-limit multicast ipv6

To configure the IPv6 multicast rate limiters, use the **mls rate-limit multicast ipv6** command. To disable the rate limiters, use the **no** form of this command.

```
mls rate-limit multicast ipv6 { connected pps [packets-in-burst] } | { rate-limiter-name { share
  { auto | target-rate-limiter } } }
```

```
no mls rate-limit multicast ipv6 { connected | rate-limiter-type }
```

### Syntax Description

<b>connected</b> <i>pps</i>	Enables and sets the rate limiters for the IPv6 multicast packets from a directly connected source; valid values are from 10 to 1000000 packets per second.
<i>packets-in-burst</i>	(Optional) Packets in burst; valid values are from 1 to 255.
<i>rate-limiter-name</i>	Rate-limiter name; valid values are <b>default-drop</b> , <b>route-ctrl</b> , <b>secondary-drop</b> , <b>sg</b> , <b>starg-bridge</b> , and <b>starg-m-bridge</b> . See the “Usage Guidelines” section for additional information.
<b>share</b>	Specifies the sharing policy for IPv6 rate limiters; see the “Usage Guidelines” section for additional information.
<b>auto</b>	Decides the sharing policy automatically.
<i>target-rate-limiter</i>	Rate-limiter name that was the first rate-limiter name programmed in the hardware for the group; valid values are <b>default-drop</b> , <b>route-ctrl</b> , <b>secondary-drop</b> , <b>sg</b> , <b>starg-bridge</b> , and <b>starg-m-bridge</b> . See the “Usage Guidelines” section for additional information.

### Defaults

If the *burst* is not set, a default of **100** is programmed for multicast cases.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

The *rate-limiter-name* argument must be a rate limiter that is not currently programmed.

The *target-rate-limiter* argument must be a rate limiter that is programmed in the hardware and must be the first rate limiter programmed for its group.

[Table 2-23](#) lists the IPv6 rate limiters and the class of traffic that each rate limiter serves.

**Table 2-23 IPv6 Rate Limiters**

Rate-Limiter ID	Traffic Classes to be Rate Limited
Connected	Directly connected source traffic
Default-drop	* (*, G/m)SSM * (*, G/m)SSM non-rpf
Route-control	* (*, FF02::X/128)
Secondary-drop	* (*, G/128) SPT threshold is infinity
SG	* (S, G) RP-RPF post-switchover * (*, FFx2/16)
Starg-bridge	* (*, G/128) SM * SM non-rpf traffic when (*, G) exists
Starg-M-bridge	* (*, G/m) SM * (*, FF/8) * SM non-rpf traffic when (*, G) does not exist

You can configure rate limiters for IPv6 multicast traffic using one of the following methods:

- Direct association of the rate limiters for a traffic class—Select a rate and associate the rate with a rate limiter. This example shows how to pick a rate of 1000 pps and 20 packets per burst and associate the rate with the **default-drop** rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 default-drop 1000 20
```

- Static sharing of a rate limiter with another preconfigured rate limiter—When there are not enough adjacency-based rate limiters available, you can share a rate limiter with an already configured rate limiter (target rate limiter). This example shows how to share the **route-ctrl** rate limiter with the **default-drop** target rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 route-ctrl share default-drop
```

If the target rate limiter is not configured, a message displays that the target rate limiter must be configured for it to be shared with other rate limiters.

- Dynamic sharing of rate limiters—If you are not sure about which rate limiter to share with, use the **share auto** keywords to enable dynamic sharing. When you enable dynamic sharing, the system picks a preconfigured rate limiter and shares the given rate limiter with the preconfigured rate limiter. This example shows how to choose dynamic sharing for the **route-ctrl** rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 route-ctrl share auto
```

## Examples

This example shows how to set the rate limiters for the IPv6 multicast packets from a directly connected source:

```
Router(config)# mls rate-limit multicast ipv6 connected 1500 20
Router(config)#
```

This example shows how to configure a direct association of the rate limiters for a traffic class:

```
Router(config)# mls rate-limit multicast ipv6 default-drop 1000 20
Router(config)#
```

This example shows how to configure the static sharing of a rate limiter with another preconfigured rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share default-drop
Router(config)#
```

This example shows how to enable dynamic sharing for the **route-cntl** rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share auto
Router(config)#
```

---

**Related Commands**

Command	Description
<a href="#">show mls rate-limit</a>	Displays information about the MLS rate limiter.

---

## mls rate-limit unicast acl

To enable and set the ACL-bridged rate limiters, use the **mls rate-limit unicast acl** command. To disable the rate limiters, use the **no** form of this command.

```
mls rate-limit unicast acl {input | output | vacl-log} {pps [packets-in-burst]}
```

```
no mls rate-limit unicast acl {input | output | vacl-log}
```

Syntax Description	input	Specifies the rate limiters for the input ACL-bridged unicast packets.
	output	Specifies the rate limiters for the output ACL-bridged unicast packets.
	vacl-log	Specifies the rate limiters for the VACL log cases.
	pps	Packets per second; see the “Usage Guidelines” section for valid values.
	packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

### Defaults

The defaults are as follows:

- **input**—Disabled.
- **output**—Disabled.
- **vacl-log**—Enabled at **2000 pps** and *packets-in-burst* is set to **1**.
- If the *packets-in-burst* is not set, **10** is programmed for unicast cases.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

The rate limiters can rate limit the packets that are punted from the data path in the hardware up to the data path in the software. The rate limiters protect the control path in the software from congestion and drop the traffic that exceeds the configured rate.

When setting the *pps*, valid values are as follows:

- ACL input and output cases—10 to 1000000 *pps*
- VACL log cases—10 to 5000 *pps*

You cannot change the **vacl-log** *packets-in-burst* keyword and argument; it is set to **1** by default.

Some cases (or scenarios) share the same hardware register. These cases are divided into the following two groups:

- Group1:
  - Egress ACL-bridged packets
  - Ingress ACL-bridged packets

- Group 2:
  - RPF failure
  - ICMP unreachable for ACL drop
  - ICMP unreachable for no-route
  - IP errors

All the components of each group use or share the same hardware register. For example, ACL-bridged ingress and egress packets use register A. ICMP-unreachable, no-route, and RPF failures use register B.

In most cases, when you change a component of a group, all the components in the group are overwritten to use the same hardware register as the first component changed. A warning message is printed out each time that an overwriting operation occurs, but only if you enable the service internal mode. The overwriting operation does not occur in these situations:

- The *pps* value is set to **0** (zero) for a particular case.
- When the ingress or egress ACL-bridged packet cases are disabled, overwriting does not occur until the cases are enabled again. If either case is disabled, the other is not affected if the remaining case is enabled. For example, if you program the ingress ACL-bridged packets with a 100-pps rate, and then you configure the egress ACL-bridged packets with a 200-pps rate, the ingress ACL-bridged packet value is overwritten to 200 pps and both the ingress and the egress ACL-bridged packets have a 200-pps rate.

### Examples

This example shows how to set the input ACL-bridged packet limiter for unicast packets:

```
Router(config)# mls rate-limit unicast acl ingress 100
Router(config)#
```

This example shows how to disable the input ACL-bridged packet limiter for unicast packets:

```
Router(config)# no mls rate-limit unicast acl ingress
Router(config)#
```

### Related Commands

Command	Description
<a href="#">show mls rate-limit</a>	Displays information about the MLS rate limiter.

## mls rate-limit unicast cef

To enable and set the CEF rate limiters, use the **mls rate-limit unicast cef** command. To disable the rate limiters, use the **no** form of this command.

```
mls rate-limit unicast cef { receive | glean } pps [packets-in-burst]
```

```
no mls rate-limit unicast cef { receive | glean }
```

Syntax Description		
	<b>receive</b>	Enables and sets the rate limiters for receive packets.
	<b>glean</b>	Enables and sets the rate limiters for ARP-resolution packets.
	<i>pps</i>	Packets per second; valid values are from 10 to 1000000 packets per second.
	<i>packets-in-burst</i>	(Optional) Packets in burst; valid values are from 1 to 255.

Defaults	
	The defaults are as follows:
	<ul style="list-style-type: none"> <li>• <b>receive</b>—Disabled.</li> <li>• <b>glean</b>—Disabled.</li> </ul>

Command Modes	
	Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Usage Guidelines	
	If you enable the CEF rate limiters, the following situations occur (if the situation that is listed is unacceptable, disable the CEF rate limiters):
	<ul style="list-style-type: none"> <li>• If a packet hits a glean/receive adjacency, the packet may be dropped instead of being sent to the software if there is an output ACL on the input VLAN and the matched entry result is deny.</li> <li>• If the matched ACL entry result is bridge, the packet is subject to egress ACL bridge rate limiting (if turned ON) instead of glean/receive rate limiting.</li> <li>• The glean/receive adjacency rate limiting is applied only if the output ACL lookup result is permit or there is no output ACLs on the input VLAN.</li> </ul>

---

**Examples**

This example shows how to set the CEF-glean limiter for the unicast packets:

```
Router(config)# mls rate-limit unicast cef glean 5000
Router(config)#
```

This example shows disable the CEF-glean limiter for the unicast packets:

```
Router(config)# no mls rate-limit unicast cef glean
Router(config)#
```

---

**Related Commands**

Command	Description
<a href="#">show mls rate-limit</a>	Displays information about the MLS rate limiter.

## mls rate-limit unicast ip

To enable and set the rate limiters for the unicast packets, use the **mls rate-limit unicast ip** command. To disable the rate limiters, use the **no** form of this command.

```
mls rate-limit unicast ip { errors | features | options | rpf-failure } pps [packets-in-burst]
```

```
mls rate-limit unicast ip icmp { redirect | unreachable { acl-drop pps } | no-route pps } [packets-in-burst]
```

```
no mls rate-limit unicast ip { errors | features | { icmp { redirect | unreachable { acl-drop | no-route } } } | options | rpf-failure } pps [packets-in-burst]
```

Syntax Description		
<b>errors</b>	Specifies rate limiting for unicast packets with IP checksum and length errors.	
<b>features</b>	Specifies rate limiting for unicast packets with software-security features in Layer 3 (for example, authorization proxy, IPsec, and inspection).	
<b>options</b>	Specifies rate limiting for unicast IPv4 packets with options.	
<b>rpf-failure</b>	Specifies rate limiting for unicast packets with RPF failures.	
<i>pps</i>	Packets per second; see the “Usage Guidelines” section for valid values.	
<i>packets-in-burst</i>	(Optional) Packets in burst; valid values are from 1 to 255.	
<b>icmp redirect</b>	Specifies rate limiting for unicast packets requiring ICMP redirect.	
<b>icmp unreachable acl-drop</b> <i>pps</i>	Enables and sets the rate limiters for the ICMP unreachables for the ACL-dropped packets.	
<b>icmp unreachable no-route</b> <i>pps</i>	Enables and sets the rate limiters for the ICMP unreachables for the FIB-miss packets.	

### Defaults

The defaults are as follows:

- If the *packets-in-burst* is not set, a default of **10** is programmed as the burst for unicast cases.
- **errors**—Enabled at **100 pps** and *packets-in-burst* set to **10**.
- **rpf-failure**—Enabled at **100 pps** and *packets-in-burst* set to **10**.
- **icmp unreachable acl-drop**—Enabled at **100 pps** and *packets-in-burst* set to **10**.
- **icmp unreachable no-route**—Enabled at **100 pps** and *packets-in-burst* set to **10**.
- **icmp redirect**—Disabled.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

To provide OAL support for denied packets, enter the **mls rate-limit unicast ip icmp unreachable acl-drop 0** command.

OAL and VACL capture are incompatible. Do not configure both features on the switch. With OAL configured, use SPAN to capture traffic.

The rate limiters can rate limit the packets that are punted from the data path in the hardware up to the data path in the software. The rate limiters protect the control path in the software from congestion and drop the traffic that exceeds the configured rate.

**Note**

When you configure an ICMP rate limiter, and an ICMP redirect occurs, exiting data traffic is dropped while the remaining traffic on the same interface is forwarded.

When setting the *pps*, the valid values are **0** and from 10 to 1000000. Setting the *pps* to **0** globally disables the redirection of the packets to the route processor. The **0** value is supported for these rate limiters:

- ICMP unreachable ACL-drop
- ICMP unreachable no-route
- ICMP redirect
- IP rpf failure

Some cases (or scenarios) share the same hardware register. These cases are divided into the following two groups:

- Group 1:
  - Egress ACL-bridged packets
  - Ingress ACL-bridged packets
- Group 2:
  - RPF failure
  - ICMP unreachable for ACL drop
  - ICMP unreachable for no-route
  - IP errors

All the components of each group use or share the same hardware register. For example, ACL-bridged ingress and egress packets use register A. ICMP-unreachable, no-route, and RPF failures use register B.

In most cases, when you change a component of a group, all the components in the group are overwritten to use the same hardware register as the first component changed. A warning message is printed out each time that an overwriting operation occurs, but only if you enable the service internal mode. The overwriting operation does not occur in these situations:

- The *pps* value is set to **0** (zero) for a particular case.
- When the ingress or egress ACL-bridged packet cases are disabled, overwriting does not occur until the cases are enabled again. If either case is disabled, the other is not affected as long as the remaining case is enabled. For example, if you program the ingress ACL-bridged packets with a 100-pps rate, and then you configure the egress ACL-bridged packets with a 200-pps rate, the ingress ACL-bridged packet value is overwritten to 200 pps and both the ingress and the egress ACL-bridged packets have a 200-pps rate.

## ■ mls rate-limit unicast ip

---

**Examples**

This example shows how to set the ICMP-redirect limiter for unicast packets:

```
Router(config)# mls rate-limit unicast ip icmp redirect 250
Router(config)#
```

---

**Related Commands**

Command	Description
<a href="#">show mls rate-limit</a>	Displays information about the MLS rate limiter.

## mls rate-limit unicast l3-features

To enable and set the Layer 3 security rate limiters for the unicast packets, use the **mls rate-limit unicast l3-features** command. To disable the rate limiters, use the **no** form of this command.

**mls rate-limit unicast l3-features** *pps* [*packets-in-burst*]

**no mls rate-limit unicast l3-features** *pps* [*packets-in-burst*]

Syntax	Description
<i>pps</i>	Packets per second; see the “Usage Guidelines” section for valid values.
<i>packets-in-burst</i>	(Optional) Packets in burst; valid values are from 1 to 255.

### Defaults

The defaults are as follows:

- Enabled at **2000** *pps* and *packets-in-burst* is set to **1**.
- If the *packets-in-burst* is not set, **10** is programmed for unicast cases.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Examples

This example shows how to set the Layer 3 security rate limiters for the unicast packets:

```
Router(config)# mls rate-limit unicast l3-features 5000
Router(config)#
```

### Related Commands

Command	Description
<a href="#">show mls rate-limit</a>	Displays information about the MLS rate limiter.

## mls rate-limit unicast vACL-log

To enable and set the VACL-log case rate limiters, use the **mls rate-limit unicast vACL-log** command. To disable the rate limiters, use the **no** form of this command.

**mls rate-limit unicast vACL-log** {*pps* [*packets-in-burst*]}

**no mls rate-limit unicast vACL-log**

Syntax Description		
	<i>pps</i>	Packets per second; see the “Usage Guidelines” section for valid values.
	<i>packets-in-burst</i>	(Optional) Packets in burst; valid values are from 1 to 255.

### Defaults

The defaults are as follows:

- Enabled at **2000** *pps* and *packets-in-burst* is set to **1**.
- If the *packets-in-burst* is not set, **10** is programmed for unicast cases.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

The rate limiters can rate limit the packets that are punted from the data path in the hardware up to the data path in the software. The rate limiters protect the control path in the software from congestion and drop the traffic that exceeds the configured rate.

When setting the *pps*, valid values are as follows:

- ACL input and output cases—10 to 1000000 *pps*
- VACL log cases—10 to 5000 *pps*

Setting the *pps* to **0** globally disables the redirection of the packets to the route processor.

You cannot change the **vACL-log** *packets-in-burst* keyword and argument; it is set to **1** by default.

Some cases (or scenarios) share the same hardware register. These cases are divided into the following two groups:

- Group 1:
  - Egress ACL-bridged packets
  - Ingress ACL-bridged packets
- Group 2:
  - RPF failure
  - ICMP unreachable for ACL drop
  - ICMP unreachable for no-route

- IP errors

All the components of each group use or share the same hardware register. For example, ACL-bridged ingress and egress packets use register A. ICMP-unreachable, no-route, and RPF failures use register B.

In most cases, when you change a component of a group, all the components in the group are overwritten to use the same hardware register as the first component changed. A warning message is printed out each time that an overwriting operation occurs, but only if you enable the service internal mode. The overwriting operation does not occur in these situations:

- The *pps* value is set to 0 (zero) for a particular case.
- When the ingress or egress ACL-bridged packet cases are disabled, overwriting does not occur until the cases are enabled again. If either case is disabled, the other is not affected if the remaining case is enabled. For example, if you program the ingress ACL-bridged packets with a 100-pps rate, and then you configure the egress ACL-bridged packets with a 200-pps rate, the ingress ACL-bridged packet value is overwritten to 200 pps and both the ingress and the egress ACL-bridged packets have a 200-pps rate.

### Examples

This example shows how to set the VACL-log case packet limiter for unicast packets:

```
Router(config)# mls rate-limit unicast vacl-log 100
Router(config)#
```

This example shows how to disable the rate limiters:

```
Router(config)# no mls rate-limit unicast vacl-log 100
Router(config)#
```

### Related Commands

Command	Description
<a href="#">show mls rate-limit</a>	Displays information about the MLS rate limiter.

## mls rp ip (global configuration mode)

To enable external systems to establish IP shortcuts to the PISA, use the **mls rp ip** command. To remove a prior entry, use the **no** form of this command.

**mls rp ip [input-acl | route-map]**

**no mls rp ip**

Syntax Description	input-acl	(Optional) Enables the IP-input access list.
	route-map	(Optional) Enables the IP-route map.

**Defaults** No shortcuts are configured.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to allow the external systems to establish IP shortcuts with IP-input access lists:

```
Router(config)# mls rp ip input-acl
Router(config)#
```

Related Commands	Command	Description
	<a href="#">mls ip</a>	Enables MLS IP for the internal router on the interface.
	<a href="#">show mls ip multicast</a>	Displays the MLS IP information.

## mls rp ip (interface configuration mode)

To enable the external systems to enable MLS IP on a specified interface, use the **mls rp ip** command. To disable MLS IP, use the **no** form of this command.

**mls rp ip**

**no mls rp ip**

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

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

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to enable the external systems to enable MLS IP on an interface:

```
Router(config-if)# mls rp ip
Router(config-if)
```

Related Commands	Command	Description
	<a href="#">mls rp ip (global configuration mode)</a>	Enables external systems to establish IP shortcuts to the PISA.
	<a href="#">show mls ip multicast</a>	Displays the MLS IP information.

## mls rp ipx (global configuration mode)

To allow the external systems to enable MLS IPX to the PISA, use the **mls rp ipx** command. To remove a prior entry, use the **no** form of this command.

**mls rp ipx [input-acl]**

**no mls rp ipx**

Syntax	Description
<b>input-acl</b>	(Optional) Enables MLS IPX and overrides ACLs.

Defaults	Description
	This command has no default settings.

Command Modes	Description
	Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Examples	Description
	This example shows how to allow the external systems to enable MLS IPX to the PISA and override ACLs:

```
Router(config)# mls rp ipx input-acl
Router(config)#
```

Related Commands	Command	Description
	<a href="#">mls rp ipx (interface configuration mode)</a>	Allows the external systems to enable MLS IPX on the interface.
	<b>show mls rp ipx</b>	Displays details for all IPX MLS interfaces on the IPX MLS router.

## mls rp ipx (interface configuration mode)

To allow the external systems to enable MLS IPX on the interface, use the **mls rp ipx** command. To disable MLS IPX on the interface, use the **no** form of this command.

**mls rp ipx**

**no mls rp ipx**

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

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

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to allow the external systems to enable MLS IPX on an interface:

```
Router(config-if)# mls rp ipx
Router(config-if)#
```

Related Commands	Command	Description
	<a href="#">mls rp ipx (global configuration mode)</a>	Allows the external systems to enable MLS IPX to the PISA.
	<b>show mls rp ipx</b>	Displays details for all IPX MLS interfaces on the IPX MLS router.

## mls rp management-interface

To enable the interface as a management interface, use the **mls rp management-interface** command. To remove a prior entry, use the **no** form of this command.

**mls rp management-interface**

**no mls rp management-interface**

---

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

---

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

---

**Command Modes** Interface configuration

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Examples** This example shows how to enable an interface as a management interface:

```
Router(config-if)# mls rp management-interface
Router(config-if)#
```

---

Related Commands	Command	Description
	<b>show mls rp</b>	Displays MLS details.

---

# mls rp nde-address

To specify the NDE address, use the **mls rp nde-address** command. To remove a prior entry, use the **no** form of this command.

**mls rp nde-address** *ip-address*

**no mls rp nde-address** *ip-address*

<b>Syntax Description</b>	<i>ip-address</i> NDE IP address.				
<b>Defaults</b>	This command has no default settings.				
<b>Command Modes</b>	Global configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(18)ZY</td> <td>Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)ZY	Support for this command was introduced.
Release	Modification				
12.2(18)ZY	Support for this command was introduced.				

<b>Usage Guidelines</b>	<p>Use the following syntax to specify an IP subnet address:</p> <ul style="list-style-type: none"> <li><i>ip-subnet-addr</i>—Short subnet address format. The trailing decimal number 00 in an IP address YY.YY.YY.00 specifies the boundary for an IP-subnet address. For example, 172.22.36.00 indicates a 24-bit subnet address (subnet mask 172.22.36.00/255.255.255.0), and 173.24.00.00 indicates a 16-bit subnet address (subnet mask 173.24.00.00/255.255.0.0). However, this format can identify only a subnet address of 8, 16, or 24 bits.</li> <li><i>ip-addr/subnet-mask</i>—Long subnet address format. For example, 172.22.252.00/255.255.252.00 indicates a 22-bit subnet address. This format can specify a subnet address of any bit number. To provide more flexibility, the <i>ip-addr</i> is a full host address, such as 172.22.253.1/255.255.252.00.</li> <li><i>ip-addr/maskbits</i>—Simplified long subnet address format. The mask bits specify the number of bits of the network masks. For example, 172.22.252.00/22 indicates a 22-bit subnet address. The <i>ip-addr</i> is a full host address, such as 193.22.253.1/22, which has the same subnet address as the <i>ip-subnet-addr</i>.</li> </ul>
-------------------------	---

**Examples** This example shows how to set the NDE address to 170.25.2.1:

```
Router(config)# mls rp nde-address 170.25.2.1
Router(config)#
```

<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>show mls rp</b></td> <td>Displays MLS details.</td> </tr> </tbody> </table>	Command	Description	<b>show mls rp</b>	Displays MLS details.
Command	Description				
<b>show mls rp</b>	Displays MLS details.				

## mls rp vlan-id

To assign a VLAN ID to the interface, use the **mls rp vlan-id** command. To remove a prior entry, use the **no** form of this command.

```
mls rp vlan-id {vlan-id}
```

```
no mls rp vlan-id
```

<b>Syntax Description</b>	<i>vlan-id</i> VLAN ID number; valid values are from 1 to 4094.				
<b>Defaults</b>	This command has no default settings.				
<b>Command Modes</b>	Interface configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Release</th> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border-bottom: 1px solid black;">12.2(18)ZY</td> <td style="border-bottom: 1px solid black;">Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)ZY	Support for this command was introduced.
Release	Modification				
12.2(18)ZY	Support for this command was introduced.				
<b>Examples</b>	<p>This example shows how to assign a VLAN ID to the interface:</p> <pre>Router(config-if)# <b>mls rp vlan-id 4</b> Router(config-if)#</pre>				
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Command</th> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Description</th> </tr> </thead> <tbody> <tr> <td style="border-bottom: 1px solid black;"><b>show mls rp</b></td> <td style="border-bottom: 1px solid black;">Displays MLS details.</td> </tr> </tbody> </table>	Command	Description	<b>show mls rp</b>	Displays MLS details.
Command	Description				
<b>show mls rp</b>	Displays MLS details.				

## mls rp vtp-domain

To link the interface to a VTP domain, use the **mls rp vtp-domain** command. To remove a prior entry, use the **no** form of this command.

**mls rp vtp-domain** *name*

**no mls rp vtp-domain** *name*

Syntax Description	<i>name</i>	VLAN domain name.
--------------------	-------------	-------------------

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

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to link the interface to a VTP domain:

```
Router(config-if)# mls rp vtp-domain EverQuest
Router(config-if)#
```

Related Commands	Command	Description
	<b>show mls rp</b>	Displays MLS details.
	<b>vtp</b>	Configures the global VTP state.

## mls sampling

To enable the sampled NetFlow and specify the sampling method, use the **mls sampling** command. To disable the sampled NetFlow, use the **no** form of this command.

**mls sampling** { **time-based** *rate* } | { **packet-based** *rate* [*interval*] }

**no mls sampling**

Syntax Description	Parameter	Description
	<b>time-based</b> <i>rate</i>	Specifies the time-based sampling rate; valid values are <b>64, 128, 256, 512, 1024, 2046, 4096,</b> and <b>8192</b> . See the “Usage Guidelines” section for additional information.
	<b>packet-based</b> <i>rate</i>	Specifies the packet-based sampling rate; valid values are <b>64, 128, 256, 512, 1024, 2046, 4096,</b> and <b>8192</b> .
	<i>interval</i>	(Optional) Sampling interval; valid values are from 8000 to 16000 milliseconds.

**Defaults** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** To enable sampling on the PFC3, you must enter the **mls sampling** command and the **mls netflow sampling** command on the appropriate interfaces. If you do not enter the **mls netflow sampling** command, NDE will not export flows.

The sampled NetFlow is supported on Layer 3 interfaces only.

You can enable the sampled NetFlow even if NDE is disabled, but no flows are exported.

With packet-based sampling, a flow with a packet count of *n* is sampled *n/m* times, where *m* is the sampling rate.

The time-based sampling is based on a preset interval for each sampling rate. [Table 5-54](#) lists the sample intervals for each rate and period.

**Table 2-24 Time-Based Sampling Intervals**

Sampling Rate	Sampling Time (milliseconds)	Export Interval (Milliseconds)
1 in 64	128	8192
1 in 128	64	8192
1 in 256	32	8192
1 in 512	16	8192

*Table 2-24 Time-Based Sampling Intervals (continued)*

Sampling Rate	Sampling Time (milliseconds)	Export Interval (Milliseconds)
1 in 1024	8	8192
1 in 2048	4	8192
1 in 4096	4	16384
1 in 8192	4	32768

**Examples**

This example shows how to enable the time-based NetFlow sampling and set the sampling rate:

```
Router(config)# mls sampling time-based 1024
Router(config)#
```

This example shows how to enable the packet-based NetFlow sampling and set the sampling rate and interval:

```
Router(config)# mls sampling packet-based 1024 8192
Router(config)#
```

**Related Commands**

Command	Description
<a href="#">mls netflow sampling</a>	Enables the sampled NetFlow on an interface.
<a href="#">show mls sampling</a>	Displays information about the sampled NDE status.

# mls switching

To enable the hardware switching, use the **mls switching** command. To disable hardware switching, use the **no** form of this command.

**mls switching**

**no mls switching**

---

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

---

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

---

**Command Modes** Global configuration

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Examples** This example shows how to enable the hardware switching:

```
Router(config)# mls switching
Router(config)#
```

This example shows how to disable the hardware switching:

```
Router(config)# no mls switching
Router(config)#
```

---

Related Commands	Command	Description
	<a href="#">mls switching unicast</a>	Enables the hardware switching of the unicast traffic for an interface.

---

# mls switching unicast

To enable the hardware switching of the unicast traffic for an interface, use the **mls switching unicast** command. To disable the hardware switching of the unicast traffic for an interface, use the **no** form of this command.

**mls switching unicast**

**no mls switching unicast**

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

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

**Command Modes** Interface configuration

Release	Modification
12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to enable the hardware switching for an interface:

```
Router(config-if)# mls switching unicast
Router(config-if)#
```

This example shows how to disable the hardware switching for an interface:

```
Router(config-if)# no mls switching unicast
Router(config-if)#
```

Command	Description
<a href="#">mls switching</a>	Enables hardware switching.

# mls verify

To enable hardware packet parsing error checks, use the **mls verify** command. To disable Layer 3 error checking in the hardware, use the **no** form of this command.

```
mls verify {ip | ipx} {checksum | {length {consistent | minimum}}} | same-address | syslog
```

```
no mls verify {ip | ipx} {checksum | {length {consistent | minimum}}} same-address | syslog
```

## Syntax Description

<b>ip</b>	Specifies the IP checksum errors.
<b>ipx</b>	Specifies the IPX checksum errors.
<b>checksum</b>	Specifies the checksum-error check.
<b>length consistent</b>	Checks the length in the header against the physical frame length.
<b>length minimum</b>	Checks the minimum packet length.
<b>same-address</b>	Checks for the packets that have equal source and destination IP addresses.
<b>syslog</b>	Specifies the syslog packet parse error traps.

## Defaults

The default settings are as follows:

- **checksum**
- **same-address** is disabled.
- **syslog** is disabled.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

The IP too-short packets are the IP packets with an IP header length or IP total length field that is smaller than 20 bytes.

When you enter the **mls verify ip length minimum** command, valid IPv4 packets are switched in the hardware only if the IP protocol fields are equal to one of the following types:

- ICMP (1)
- IGMP (2)
- IP (4)
- TCP (6)
- UDP (17)
- IPv6 (41)

- GRE (47)
- SIPP-ESP (50)

When you enter the **no mls verify ip length minimum** command, too-short packets are switched in the hardware. The too-short packets that have IP protocol = 6 (TCP) are sent to the software.

To prevent packets with the same source and destination IP address from being switched in the hardware, use the **mls verify ip same-address** command.

---

## Examples

This example shows how to enable Layer 3 error checking in the hardware:

```
Router(config)# mls verify ip checksum
Router(config)#
```

This example shows how to disable Layer 3 error checking in the hardware:

```
Router(config)# no mls verify ip checksum
Router(config)#
```

This example shows how to prevent packets with the same source and destination IP address from being switched in the hardware:

```
Router(config)# mls verify ip same-address
Router(config)#
```

# mobility

To configure the wireless mGRE tunnels, use the **mobility** command. To return to the default settings, use the **no** form of this command.

**mobility** {**network-id** *id*} | {**tcp adjust-mss**}

**mobility** [**trust** | **broadcast**]

Syntax Description	network-id <i>id</i>	Specifies the wireless network ID for the mGRE tunnel; valid values are from 1 to 4095.
	<b>tcp adjust-mss</b>	Adjusts the MSS value in TCP SYN and TCP ACK on the access points automatically.
	<b>trust</b>	(Optional) Specifies the trusted network.
	<b>broadcast</b>	(Optional) Specifies that the mGRE tunnel convert the NBMA to the BMA.

**Defaults** Untrusted network

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command is supported on Catalyst 6500 series switches that are configured with a WLSM only. The **tcp adjust-mss** keywords are supported on mGRE tunnel interfaces only. You can enter the **ip tcp adjust-mss** *value* command to change the TCP MSS to a lower value. A trusted network can use DHCP or a static IP address. An untrusted network supports only DHCP clients.

**Examples** This example shows how to specify the network identification number for the mGRE tunnel:

```
Router (config-if)# mobility network-id 200
Router (config-if)#
```

This example shows how to specify the trusted network:

```
Router (config-if)# mobility trust
Router (config-if)#
```

This example shows how to specify that the mGRE tunnel convert the NBMA to the BMA:

```
Router (config-if)# mobility broadcast
Router (config-if)#
```

This example shows how to adjust the MSS value in TCP SYN and TCP ACK on the access points automatically:

```
Router (config-if)# mobility tcp adjust-mss
Router (config-if)#
```

---

**Related Commands**

Command	Description
<b>ip tcp adjust-mss</b>	Adjusts the MSS value of TCP SYN packets going through a router.
<b>show mobility</b>	Displays information about the Layer 3 mobility and the wireless network.

# mode

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

**mode** { **rpr** | **rpr-plus** | **sso** }

Syntax Description	Parameter	Description
	<b>rpr</b>	Specifies RPR mode.
	<b>rpr-plus</b>	Specifies RPR+ mode.
	<b>sso</b>	Specifies SSO mode.

## Defaults

The defaults are as follows:

- SSO mode if the system is not configured for redundancy and the active and standby supervisor engines have the same image.
- RPR mode if different versions are installed.
- If redundancy is enabled, the default is the mode that you have configured.

## Command Modes

Redundancy configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

The **rpr-plus** keywords are not supported by the Supervisor Engine 32 PISA.

NSF with SSO redundancy mode supports IPv4. NSF with SSO redundancy mode does not support IPv6, IPX, and MPLS.

If you have configured MPLS on the Catalyst 6500 series switch with redundant supervisor engines, you must configure the Catalyst 6500 series switch in RPR mode. The switch should not be running in the default mode of SSO.

Enter the **redundancy** command in global configuration mode to enter redundancy configuration mode. You can enter the **mode** command within redundancy configuration mode.

The standby supervisor engine reloads on any change of mode and begins to work in the current mode.

## Examples

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

```
Router(config)# redundancy
Router(config-red)# mode sso
Router(config-red)#
```

Related Commands	Command	Description
	<b>redundancy</b>	Enters redundancy configuration mode.
	<b>redundancy force-switchover</b>	Forces a switchover from the active to the standby supervisor engine.
	<b>route-converge-interval</b>	Configures the time interval after which the old FIB entries are purged.
	<b>show redundancy</b>	Displays RF information.
	<b>show running-config</b>	Displays the status and configuration of the module or Layer 2 VLAN.

## mode dot1q-in-dot1q access-gateway

To enable a Gigabit Ethernet WAN interface to act as a gateway for QinQ VLAN translation, use the **mode dot1q-in-dot1q access-gateway** command. To disable the QinQ VLAN translation on the interface, use the **no** form of this command.

**mode dot1q-in-dot1q access-gateway**

**no mode dot1q-in-dot1q access-gateway**

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

**Defaults** Disabled

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command is supported on the Gigabit Ethernet WAN interfaces on Catalyst 6500 series switches that are configured with an OSM-2+4GE-WAN+ OSM module only.

802.1Q provides a trunking option that tags packets with two VLAN tags to allow multiple VLANs to be trunked together across an intermediate network. This use of a double-tagged tunnel is also referred to as QinQ tunneling.

The **mode dot1q-in-dot1q access-gateway** command enhances QinQ tunneling by tagging packets with two VLAN tags to allow multiple VLANs to be trunked together across an intermediate network. A double-tagged tunnel performs the following functions:

- Switches packets that are tagged with two 802.1Q VLAN tags to a destination service that is based on a combination of VLAN tags.
- Supports traffic shaping based on the VLAN tags.
- Copies the 802.1P prioritization bits (P bits) from the inner (customer) VLAN tag to the outer (service provider) VLAN tag.

You can also combine multiple GE-WAN interfaces into a virtual port-channel interface to enable QinQ link bundling. Combining the interfaces not only simplifies the configuration but allows the GE-WAN OSM to load balance the PE VLANs among the physical interfaces that are members of the bundle. In addition, if one interface member of the link bundle goes down, its PE VLANs are automatically reallocated to the other members of the bundle.



**Note** You must remove all IP addresses that have been configured on the interface before using the **mode dot1q-in-dot1q access-gateway** command.

After configuring the **mode dot1q-in-dot1q access-gateway** command, use the **bridge-domain (subinterface configuration)** command to configure the VLAN mapping to be used on each subinterface.

**Caution**

Using the **mode dot1q-in-dot1q access-gateway** command on an interface automatically deletes all the subinterfaces that might be configured on the interface. It also releases any internal VLANs that might have been previously used on the interface and its subinterfaces, allowing them to be reused for QinQ translation. Using the **no** form of the command deletes all subinterfaces and releases any VLANs that are currently being used by the interface and subinterface. We recommend that you save the interface configuration before entering the **mode dot1q-in-dot1q access-gateway** command.

**Note**

Port-channel interface counters (as shown by the **show counters interface port-channel** and **show interface port-channel counters** commands) are not supported for channel groups that are using GE-WAN interfaces for QinQ link bundling. The **show interface port-channel {number | number.subif}** command (without the **counters** keyword) is supported, however.

**Tip**

The **mls qos trust** command has no effect on a GE-WAN interface or port-channel group that has been configured with the **mode dot1q-in-dot1q access-gateway** command. These interfaces and port channels always trust the VLAN CoS bits in this configuration.

**Examples**

This example shows a typical configuration for the **mode dot1q-in-dot1q access-gateway** command:

```
Router# configure terminal
Router(config)# interface GE-WAN 4/1
Router(config-if)# mode dot1q-in-dot1q access-gateway
Router(config-if)#
```

This example shows the system message that appears when you try to configure the **mode dot1q-in-dot1q access-gateway** command without first removing the IP address configuration:

```
Router# configure terminal
Router(config)# interface GE-WAN 3/0
Router(config-if)# mode dot1q-in-dot1q access-gateway

% interface GE-WAN3/0 has IP address 495146814001404
configured! Please remove the IP address before configuring
'mode dot4q-in-dot4q access-gateway' on this interface!

Router(config-if)# no ip address 192.168.100.101 255.255.255
Router(config-if)# mode dot1q-in-dot1q access-gateway
Router(config-if)#
```

This example shows how to disable QinQ mapping on an interface by using the **no** form of the **mode dot1q-in-dot1q access-gateway** command. In addition, this command automatically removes all subinterfaces on the interface and all of the subinterface QinQ mappings (configured with the **bridge-domain (subinterface configuration)** command) and service policies.

```
Router# configure terminal
Router(config)# interface GE-WAN 3/0
Router(config-if)# no mode dot1q-in-dot1q access-gateway
Router(config-if)#
```

## mode dot1q-in-dot1q access-gateway

This example shows a virtual port-channel interface that was created and assigned with two GE-WAN interfaces. The **mode dot1q-in-dot1q access-gateway** command is then enabled on the port-channel interface to allow it to act as a QinQ link bundle:

```
Router(config)# interface port-channel 20
Router(config-if)# interface GE-WAN 3/0
Router(config-if)# port-channel 20 mode on
Router(config-if)# interface GE-WAN 3/1
Router(config-if)# port-channel 20 mode on
Router(config-if)# interface port-channel 20
Router(config-if)# no ip address
Router(config-if)# mode dot1q-in-dot1q access-gateway
Router(config-if)#
```

This example shows the error message that appears if you attempt to enable QinQ translation on a port-channel interface that contains one or more invalid interfaces:

```
Router# configure terminal
Router(config)# interface port-channel 30
7600-5(config-if)# mode dot1q-in-dot1q access-gateway

% 'mode dot4q-in-dot4q access-gateway' is not supported on Port-channel30
% Port-channel30 contains 5 Layer 5 Gigabit Ethernet interface(s)

Router(config-if)#
```

## Related Commands

Command	Description
<b>bridge-domain (subinterface configuration)</b>	Binds a PVC to the specified <i>vlan-id</i> .
<b>class-map</b>	Accesses the QoS class map configuration mode to configure QoS class maps.
<b>policy-map</b>	Accesses QoS policy-map configuration mode to configure the QoS policy map.
<b>service-policy</b>	Attaches a policy map to an interface.
<b>set cos cos-inner (policy-map configuration)</b>	Sets the 802.1Q prioritization bits in the trunk VLAN tag of a QinQ-translated outgoing packet with the priority value from the inner customer-edge VLAN tag.

## monitor event-trace (EXEC)

To control the event trace function for a specified Cisco IOS software subsystem component, use the **monitor event-trace** command.

```
monitor event-trace all-traces { { continuous [cancel] } | { dump [merged] [pretty] } }
```

```
monitor event-trace l3 { clear | { continuous [cancel] } | disable | { dump [pretty] } | enable | { interface type mod/port } | one-shot }
```

```
monitor event-trace spa { clear | { continuous [cancel] } | disable | { dump [pretty] } | enable | one-shot }
```

```
monitor event-trace subsys { clear | { continuous [cancel] } | disable | { dump [pretty] } | enable | one-shot }
```

Syntax Description		
<b>all-traces</b>		Displays the configured merged-event traces.
<b>continuous</b>		Displays the latest event trace entries continuously.
<b>cancel</b>	(Optional)	Cancels the continuous display of latest trace entries.
<b>dump</b>		Writes the event trace results to the file configured using the <b>monitor event-trace (global configuration)</b> command.
<b>merged</b>	(Optional)	Dumps the entries in all event traces sorted by time.
<b>pretty</b>	(Optional)	Saves the event trace message in an ASCII format.
<b>l3</b>		Displays information about the Layer 3 trace.
<b>clear</b>		Clears the trace.
<b>disable</b>		Turns off event tracing for the specified component.
<b>enable</b>		Turns on event tracing for the specified component.
<b>interface</b> <i>type mod/port</i>		Specifies the interface to be logged.
<b>one-shot</b>		Clears any existing trace information from the memory, starts event tracing again, and disables the trace when the trace reaches the size specified using the <b>monitor event-trace (global configuration)</b> command.
<b>spa</b>		Displays information about the SPA trace.
<b>subsys</b>		Displays information about the initial trace of the subsystem.

**Defaults** Trace information is saved in a binary format.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

Use the **monitor event-trace** (EXEC) command to control what, when, and how event trace data is collected. Use this command after you have configured the event trace functionality on the networking device using the **monitor event-trace (global configuration)** command.

The trace messages are saved in a binary format.

**Note**

The amount of data collected from the trace depends on the trace message size configured using the **monitor event-trace (global configuration)** command for each instance of a trace.

Cisco IOS software allows for the subsystem components to define whether support for event tracing is enabled or disabled at boot. You can enable or disable event tracing in two ways: using the **monitor event-trace** (EXEC) command or using the **monitor event-trace (global configuration)** command. To enable event tracing again, you would enter the **enable** form of either of these commands.

To determine whether a subsystem has enabled or disabled event tracing, use the **monitor event-trace ?** command to get a list of software components that support event tracing. To determine whether event tracing is enabled by default for the subsystem, use the **show monitor event-trace** command to view trace messages.

Use the **show monitor event-trace** command to display trace messages.

Use the **monitor event-trace component dump** command to save trace message information for a single event. By default, trace information is saved in a binary format. If you want to save trace messages in an ASCII format, possibly for additional application processing, use the **monitor event-trace component dump pretty** command.

To write the trace messages for all events currently enabled on a networking device to a file, enter the **monitor event-trace dump-file (global configuration)** command.

To configure the file where you want to save trace information, use the **monitor event-trace (global configuration)** command.

**Examples**

This example shows how to stop event tracing, clear the current memory, and reenables the trace function for the SPA component. This example assumes that the tracing function is configured and enabled on the networking device.

```
Router# monitor event-trace spa disable
Router# monitor event-trace spa clear
Router# monitor event-trace spa enable
```

This example shows how you can use the **one-shot** keyword to accomplish the same function as the previous example except that you do not have to enter as many commands. Once the size of the trace message file has been exceeded, the trace is terminated.

```
Router# monitor event-trace spa one-shot
Router#
```

This example shows how to write the trace messages for an event in a binary format. The trace messages for the IPC component are written to a file as follows:

```
Router# monitor event-trace ipc dump
Router#
```

This example shows how to write the trace messages for an event in an ASCII format. In this example, the trace messages for the MBUS component are written to a file.

```
Router# monitor event-trace mbus dump pretty
Router#
```

---

**Related Commands**

Command	Description
<a href="#">monitor event-trace (global configuration)</a>	Configures event tracing for a specified Cisco IOS software subsystem component.
<b>show monitor event-trace</b>	Displays event trace messages for Cisco IOS software subsystem components.

---

## monitor event-trace (global configuration)

To configure event tracing for a specified Cisco IOS software subsystem component, use the **monitor event-trace** (global) command. To change the default setting to enable or disable event tracing, see the “Usage Guidelines” section for this command.

**monitor event-trace all-traces dump-file** *filename*

**monitor event-trace l3** { **disable** | **dump-file** *filename* | **enable** | **size** *number* | { **stacktrace** [*depth*] } }

**monitor event-trace sequence-number**

**monitor event-trace spa** { **disable** | **dump-file** *filename* | **enable** | **size** *number* | { **stacktrace** [*depth*] } }

**monitor event-trace stacktrace**

**monitor event-trace subsys** { **disable** | **dump-file** *filename* | **enable** | **size** *number* | { **stacktrace** [*depth*] } }

**monitor event-trace timestamps** [{ **datetime** [**localtime**] [**msec**] [**show-timezone**] } | **uptime**]

### Syntax Description

<b>dump-file</b> <i>filename</i>	Specifies the URL to store the dump file containing the merged traces.
<b>l3</b>	Displays information about the Layer 3 trace.
<b>disable</b>	Turns off event tracing.
<b>enable</b>	Turns on event tracing.
<b>size</b> <i>number</i>	Sets the number of messages that can be written to memory for a single instance of a trace; valid values are from 1 to 65536 messages.
<b>stacktrace</b>	Displays the stack trace stored with event trace entries.
<i>depth</i>	(Optional) Trace call stack at tracepoints; valid values are from 1 to 16.
<b>sequence-number</b>	Displays the event trace entries with a sequence number.
<b>spa</b>	Displays information about the SPA trace.
<b>subsys</b>	Displays information about the initial trace of the subsystem.
<b>timestamps</b>	Displays information about the format of event trace time stamps.
<b>datetime</b>	(Optional) Displays information about the format of event trace time stamps.
<b>localtime</b>	(Optional) Displays information about the format of event trace time stamps and includes the date and time.
<b>msec</b>	(Optional) Includes milliseconds in the time stamp.
<b>show-timezone</b>	(Optional) Displays information about the format of event trace time stamps and includes time zone information.
<b>uptime</b>	(Optional) Displays time-stamped information about the system uptime.

### Defaults

Enabled or disabled depending on the software component.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines



#### Note

Event tracing is intended for use as a software diagnostic tool and should be configured only under the direction of a TAC representative. In Cisco IOS software images that do not provide subsystem support for the event trace function, the **monitor event-trace (global configuration)** command is not available.

Cisco IOS software allows the subsystem components to define whether support for event tracing is enabled or disabled by default. The command interface for event tracing allows users to change the default two ways: using the **monitor event-trace (EXEC)** command or using the **monitor event-trace (global configuration)** command.

Additionally, default settings do not show up in the configuration file. If the subsystem software enables event tracing by default, the **monitor event-trace component enable** command will not show up in the configuration file of the networking device; however, disabling event tracing that has been enabled by default by the subsystem will create a line in the configuration file.



#### Note

The amount of data collected from the trace depends on the trace message size configured using the **monitor event-trace (global configuration)** command for each instance of a trace.

When the number of event trace messages in memory exceeds the size, new messages will begin to overwrite the older messages in the file.

The maximum *filename* length (path and filename) is 100 characters and the path can point to flash memory on the networking device or to a TFTP or FTP server.

To determine whether a subsystem has enabled or disabled event tracing, use the **monitor event-trace ?** command to get a list of software components that support event tracing.

To determine whether event tracing is enabled by default for the subsystem, use the **show monitor event-trace** command to view trace messages.

To specify the trace call stack at tracepoints, you must clear the trace buffer first.

## ■ monitor event-trace (global configuration)

**Examples**

This example shows how to stop event tracing, clear the current memory, and reenable the trace function for the SPA component. This example assumes that the tracing function is configured and enabled on the networking device.

```
Router(config)# monitor event-trace spa disable
Router(config)# monitor event-trace spa clear
Router(config)# monitor event-trace spa enable
```

**Related Commands**

Command	Description
<b>monitor event-trace (EXEC)</b>	Controls the event trace function for a specified Cisco IOS software subsystem component.
<b>show monitor event-trace</b>	Displays event trace messages for Cisco IOS software subsystem components.

## monitor permit-list

To configure a destination port permit list or add to an existing destination port permit list, use the **monitor permit-list** command. To delete from or clear an existing destination port permit list, use the **no** form of this command.

**monitor permit-list**

**monitor permit-list destination** {**interface** *type*} {*slot/port[-port]* [, *type slot/port - port*]

**no monitor permit-list**

**no monitor permit-list destination** {**interface** *type*} {*slot/port[-port]* [, *type slot/port - port*]

Syntax Description	Parameter	Description
	<b>destination</b>	Specifies a destination port.
	<b>interface</b> <i>type</i>	Specifies the interface type; valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , or <b>tengigabitethernet</b> .
	<i>slot/port</i>	Slot and port number.
	<i>-port</i>	(Optional) Range of ports.
	,	(Optional) Additional interface type and range of ports.

**Defaults** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** To prevent accidental configuration of ports as destinations, you can create a permit list of the ports that are valid for use as destinations. With a destination port permit list configured, you can only configure the ports in the permit list as destinations.

**Examples** This example shows how to configure a destination port permit list that includes Gigabit Ethernet ports 5/1 through 5/4 and 6/1:

```
Router# configure terminal
Router(config)# monitor permit-list
Router(config)# monitor permit-list destination interface gigabitethernet 5/1-4,
gigabitethernet 6/1
```

## ■ monitor permit-list

Related Commands	Command	Description
	<a href="#">show monitor permit-list</a>	Displays the permit-list state and interfaces configured.

# monitor session

To start a new ERSPAN, SPAN, or RSPAN session, add or delete interfaces or VLANs to or from an existing session, filter ERSPAN, SPAN, or RSPAN traffic to specific VLANs, or delete a session, use the **monitor session** command. To remove one or more source or destination interfaces from the session, remove a source VLAN from the session, or delete a session, use the **no** form of this command.

```
monitor session session source { {interface type} | {vlan vlan-id} [rx | tx | both]} |
  {remote vlan rspan-vlan-id}
```

```
monitor session session destination { {interface type} | {vlan vlan-id} | {remote vlan vlan-id} |
  {analysis-module slot-number} | {data-port port-number}}
```

```
monitor session session-number filter vlan vlan-range
```

```
monitor session servicemodule mod-list
```

```
monitor session session-number type {erspan-source | erspan-destination}
```

```
no monitor session { {range session-range} | local | remote | all | session}
```

```
no monitor session session source { {interface type} | {vlan vlan-id} [rx | tx | both]} |
  {remote vlan rspan-vlan-id}
```

```
no monitor session session destination { {interface type} | {vlan vlan-id} | {remote vlan vlan-id}
  | {analysis-module slot-number} | {data-port port-number}}
```

## Syntax Description

<i>session</i>	Number of the SPAN session; valid values are from 1 to 66.
<b>source</b>	Specifies the SPAN source.
<b>interface</b> <i>type</i>	Specifies the interface type; see the “Usage Guidelines” section for formatting information.
<b>vlan</b> <i>vlan-id</i>	Specifies the VLAN ID; valid values are from 1 to 4094.
<b>rx</b>	(Optional) Specifies the monitor-received traffic only.
<b>tx</b>	(Optional) Specifies the monitor-transmitted traffic only.
<b>both</b>	(Optional) Specifies the monitor-received and monitor-transmitted traffic.
<b>remote vlan</b> <i>rspan-vlan-id</i>	Specifies the RSPAN VLAN as a destination VLAN.
<b>destination</b>	Specifies the SPAN-destination interface.
<b>analysis-module</b> <i>slot-number</i>	Specifies the network analysis module number; see the “Usage Guidelines” section for additional information.
<b>data-port</b> <i>port-number</i>	Specifies the data-port number; see the “Usage Guidelines” section for additional information.
<b>filter vlan</b> <i>vlan-range</i>	Limits SPAN-source traffic to specific VLANs.
<b>servicemodule</b> <i>mod-list</i>	Specifies service modules. (Optional) List of service module numbers.
<b>type</b> <b>erspan-source</b>	Enters the ERSPAN source-session configuration mode; see the <b>monitor session type</b> command for additional information.

<b>type</b>	Enters the ERSPAN destination-session configuration mode; see the
<b>erspan-destination</b>	<b>monitor session type</b> command for additional information.
<b>range</b> <i>session-range</i>	Specifies the range of sessions.
<b>local</b>	Specifies the local session.
<b>remote</b>	Specifies the remote session.
<b>all</b>	Specifies all sessions.

**Defaults**

The defaults are as follows:

- **both.**
- **servicemodule**—All service modules are allowed to use the SPAN servicemodule session.

**Command Modes**

Global configuration

**Command History**

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines



## Note

Be careful when configuring SPAN-type source ports that are associated to SPAN-type destination ports because you do not configure SPAN on high-traffic interfaces. If you configure SPAN on high-traffic interfaces, you may saturate replication engines and interfaces. To configure SPAN-type source ports that are associated to SPAN-type destination ports, enter the **monitor session session source** `{{interface type} | {{vlan vlan-id} [rx | tx | both]} | {remote vlan rspan-vlan-id}}` command.

Use these formatting guidelines when configuring monitor sessions:

- *interface* and *single-interface* formats are *type slot/port*; valid values for *type* are **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**.
- An *interface-list* is a list of interfaces that are separated by commas. Insert a space before and after each comma as shown in this example:

*single-interface , single-interface , single-interface ...*

- An *interface-range* is a range of interfaces that are separated by dashes. Insert a space before and after each dash. To enter multiple ranges, separate each range with a comma as shown in this example:

*type slot/first-port - last-port*

- A *mixed-interface-list* is a mixed list of interfaces. Insert a space before and after each dash and comma as shown in this example:

*single-interface, interface-range , ... in any order.*

- A *single-vlan* is an ID number of a single VLAN; valid values are from 1 to 4094.
- A *vlan-list* is a list of VLAN IDs that are separated by commas. An example is shown as follows:

*single-vlan , single-vlan , single-vlan ...*

- A *vlan-range* is a range of VLAN IDs that are separated by dashes. An example is shown as follows:

*first-vlan-ID - last-vlan-ID*

- A *mixed-vlan-list* is a mixed list of VLAN IDs. Insert a space before and after each dash. To enter multiple ranges, separate each VLAN ID with a comma as shown in this example:

*single-vlan , vlan-range , ... in any order*

The **analysis-module slot-number** and the **data-port port-number** keywords and arguments are supported on Network Analysis Modules only.

The number of valid values for **port-channel number** are a maximum of 64 values ranging from 1 to 256.

You cannot share the destination interfaces among SPAN sessions. For example, a single destination interface can belong to one SPAN session only and cannot be configured as a destination interface in another SPAN session.

The local SPAN, RSPAN, and ERSPAN session limits are as follows:

Total Sessions	Local SPAN, RSPAN Source, or ERSPAN Source Sessions	RSPAN Destination Sessions	ERSPAN Destination Sessions
66	2 (ingress or egress or both)	64	23

The local SPAN, RSPAN, and ERSPAN source and destination limits are as follows:

	In Each Local SPAN Session	In Each RSPAN Source Session	In Each ERSPAN Source Session	In Each RSPAN Destination Session	In Each ERSPAN Destination Session
Egress or ingress and egress sources				—	—
	128	128	128		
Ingress sources				—	—
	128	128	128		
RSPAN and ERSPAN destination session sources	—	—	—	1 RSPAN VLAN	1 IP address
Destinations per session	64	1 RSPAN VLAN	1 IP address	64	64

A particular SPAN session can either monitor the 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 get an error. You also get an error if you configure a SPAN session with a source VLAN and then try to add a source interface to that session. You must first clear any sources for a SPAN session before switching to another type of source.

If you enter the **filter** keyword on a monitored trunk interface, only traffic on the set of specified VLANs is monitored.

The port-channel interfaces display in the list of **interface** options if you have them configured. The VLAN interfaces are not supported. However, you can span a particular VLAN by entering the **monitor session session source vlan vlan-id** command.

The **show monitor** command displays the SPAN servicemodule session only if it is allocated in the system. It also displays a list of allowed modules and a list of active modules that can use the servicemodule session.

Only the **no** form of the **monitor session servicemodule** command is displayed when you enter the **show running-config** command.

If no module is allowed to use the servicemodule session, the servicemodule session is automatically deallocated. If at least one module is allowed to use the servicemodule session and at least one module is online, the servicemodule session is automatically allocated.

If you allow or disallow a list of modules that are not service modules from using the servicemodule session, there will be no effect on the allocation or deallocation of the servicemodule session. Only the list of modules is saved in the configuration.

If you disable the SPAN servicemodule session with the **no monitor session servicemodule** command, allowing or disallowing a list of modules from using the servicemodule session has no effect on the allocation or deallocation of the servicemodule session. Only the list of modules is saved in the configuration.

The **monitor session servicemodule** command is accepted even if there are no modules physically inserted in any slot.

## Examples

This example shows how to configure multiple sources for a session:

```
Router(config)# monitor session 2 source interface fastethernet 5/15 , 7/3 rx
Router(config)# monitor session 2 source interface gigabitethernet 1/2 tx
Router(config)# monitor session 2 source interface port-channel 102
```

```
Router(config)# monitor session 2 source filter vlan 2 - 3
Router(config)# monitor session 2 destination remote vlan 901
```

This example shows how to configure an RSPAN destination in the final switch (RSPAN destination session):

```
Router(config)# monitor session 8 source remote vlan 901
Router(config)# monitor session 8 destination interface fastethernet 1/2 , 2/3
```

This example shows how to clear the configuration for sessions 1 and 2:

```
Router(config)# no monitor session 1 - 2
Router(config)#
```

This example shows how to clear the configuration for all sessions:

```
Router(config)# no monitor session all
Router(config)#
```

This example shows how to clear the configuration for all remote sessions:

```
Router(config)# no monitor session remote
Router(config)#
```

This example shows how to allow a list of modules to use the SPAN servicemodule session:

```
Router(config)# monitor session servicemodule module 1-2
Router(config)#
```

This example shows how to disallow a list of modules from using the SPAN servicemodule session:

```
Router(config)# no monitor session servicemodule module 1-2
Router(config)#
```

## Related Commands

Command	Description
<a href="#">remote-span</a>	Configures a VLAN as an RSPAN VLAN.
<a href="#">show monitor session</a>	Displays information about the ERSPAN, SPAN, and RSPAN sessions.

## monitor session type

To create an ERSPAN source session number or enter the ERSPAN session configuration mode for the session, use the **monitor session type** command. To remove one or more source or destination interfaces from the ERSPAN session, use the **no** form of this command.

**monitor session** *erspan-session-number* **type** { **erspan-destination** | **erspan-source** }

**no monitor session** *erspan-session-number* **type** { **erspan-destination** | **erspan-source** }

### Syntax Description

<i>erspan-session-number</i>	Number of the SPAN session; valid values are from 1 to 66.
<b>type erspan-destination</b>	Specifies the ERSPAN destination-session configuration mode.
<b>type erspan-source</b>	Specifies the ERSPAN source-session configuration mode.

### Defaults

This command has no default settings.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

ERSPAN is supported on hardware revision 3.2 or higher. Enter the **show module version | include WS-SUP720-BASE** command to display the hardware revision.

ERSPAN traffic is GRE-encapsulated SPAN traffic that can only be processed by an ERSPAN destination session.

All ERSPAN source sessions on a switch must use the same source IP address. You enter the **origin ip address** command to configure the IP address for the ERSPAN source sessions.

All ERSPAN destination sessions on a switch must use the same IP address. You enter the **ip address** command to configure the IP address for the ERSPAN destination sessions. If the ERSPAN destination IP address is not a Supervisor Engine 32 PISA (for example, it is a network sniffer), the traffic arrives with the GRE and RSPAN headers/encapsulation intact.

The ERSPAN source session destination IP address, which must be configured on an interface on the destination switch, is the source of traffic that an ERSPAN destination session sends to the destination ports. You configure the same address in both the source and destination sessions with the **ip address** command.

The ERSPAN ID differentiates the ERSPAN traffic arriving at the same destination IP address from different ERSPAN source sessions.

The local ERSPAN session limits are as follows:

- Total sessions—66
- Source sessions—2 (ingress or egress or both)
- Destination sessions—23

The **monitor session type** command creates a new ERSPAN session or allows you to enter the ERSPAN session configuration mode. ERSPAN uses separate source and destination sessions. You configure the source and destination sessions on different switches. The ERSPAN session configuration mode prompts are as follows:

- Router(config-mon-erspan-src)—Indicates the ERSPAN source session configuration mode.
- Router(config-mon-erspan-src-dst)—Indicates the ERSPAN source session destination configuration mode.
- Router(config-mon-erspan-dst)—Indicates the ERSPAN destination session configuration mode.
- Router(config-mon-erspan-dst-src)—Indicates the ERSPAN destination session source configuration mode

Table 2-25 lists the ERSPAN destination session configuration mode syntaxes.

Table 2-25 ERSPAN Destination Session Configuration Mode Syntaxes

Syntax	Description
<b>Global Configuration Mode</b>	
<b>monitor session</b> <i>erspan-destination-session-number</i> <b>type</b> <b>erspan-destination</b>	Enters ERSPAN destination session configuration mode and changes the prompt to the following:  Router(config-mon-erspan-dst)#
<b>Destination Session Configuration Mode</b>	
<b>description</b> <i>session-description</i>	(Optional) Describes the ERSPAN destination session.
<b>shutdown</b>	(Optional) (Default) Inactivates the ERSPAN destination session.
<b>no shutdown</b>	Activates the ERSPAN destination session.
<b>destination</b> { <i>single-interface</i>   <i>interface-list</i>   <i>interface-range</i>   <i>mixed-interface-list</i> }	Associates the ERSPAN destination session number with the destination ports.
<b>source</b>	Enters ERSPAN destination session source configuration mode and changes the prompt to the following:  Router(config-mon-erspan-dst-src)#
<b>Destination Session Source Configuration Mode</b>	
<b>ip address</b> <i>ip-address</i> [ <b>force</b> ]	Configures the ERSPAN flow destination IP address, which must also be configured on an interface on the destination switch and be entered in the ERSPAN destination session configuration.
<b>erspan-id</b> <i>erspan-flow-id</i>	Configures the ID number used by the destination and destination sessions to identify the ERSPAN traffic.
<b>vrf</b> <i>vrf-name</i>	(Optional) Configures the VRF name of the packets in the ERSPAN traffic.

Table 2-26 lists the ERSPAN source session configuration mode syntaxes.

Table 2-26 ERSPAN Source Session Configuration Mode Syntaxes

Syntax	Description
<b>Global Configuration Mode</b>	
<b>monitor session</b> <i>erspan-source-session-number</i> <b>type</b> <b>erspan-source</b>	Enters ERSPAN source session configuration mode and changes the prompt to the following:  Router (config-mon-erspan-src) #
<b>Source Session Configuration Mode</b>	
<b>description</b> <i>session-description</i>	(Optional) Describes the ERSPAN source session.
<b>shutdown</b>	(Optional) (Default) Inactivates the ERSPAN source session.
<b>no shutdown</b>	Activates the ERSPAN source session.
<b>source</b> {{ <i>single-interface</i>   <i>interface-list</i>   <i>interface-range</i>   <i>mixed-interface-list</i>   <i>single-vlan</i>   <i>vlan-list</i>   <i>vlan-range</i>   <i>mixed-vlan-list</i> } [ <b>rx</b>   <b>tx</b>   <b>both</b> ]	Associates the ERSPAN source session number with the source ports or VLANs, and selects the traffic direction to be monitored.
<b>filter</b> { <i>single-vlan</i>   <i>vlan-list</i>   <i>vlan-range</i>   <i>mixed-vlan-list</i> }	(Optional) Configures source VLAN filtering when the ERSPAN source is a trunk port.
<b>destination</b>	Enters ERSPAN source session destination configuration mode and changes the prompt to the following:  Router (config-mon-erspan-src-dst) #
<b>Source Session Destination Configuration Mode</b>	
<b>ip address</b> <i>ip-address</i>	Configures the ERSPAN flow destination IP address, which must also be configured on an interface on the destination switch and be entered in the ERSPAN destination session configuration.
<b>erspan-id</b> <i>erspan-flow-id</i>	Configures the ID number used by the source and destination sessions to identify the ERSPAN traffic.
<b>origin ip address</b> <i>ip-address</i>	Configures the IP address used as the source of the ERSPAN traffic.
<b>ip</b> {{ <b>ttl</b> <i>tvl-value</i> }   { <b>prec</b> <i>ipp-value</i> }   { <b>dscp</b> <i>dscp-value</i> } }	(Optional) Configures the following packet values in the ERSPAN traffic: <ul style="list-style-type: none"> <li>• <b>ttl</b> <i>tvl-value</i>—IP time-to-live (TTL) value</li> <li>• <b>prec</b> <i>ipp-value</i>—IP-precedence value</li> <li>• <b>dscp</b> <i>dscp-value</i>—IP-precedence value</li> </ul>
<b>vrf</b> <i>vrf-name</i>	(Optional) Configures the VRF name of the packets in the ERSPAN traffic.

When you configure the monitor sessions, follow these syntax guidelines:

- *erspan-destination-span-session-number* can range from 1 to 66.
- *single-interface* is **interface type slot/port**; *type* is **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**.

- *interface-list* is *single-interface* , *single-interface* , *single-interface* ...



**Note** In lists, you must enter a space before and after the comma. In ranges, you must enter a space before and after the dash.

- *interface-range* is **interface** *type slot/first-port - last-port* .
- *mixed-interface-list* is, in any order, *single-interface* , *interface-range* , ...
- *erspan-flow-id* can range from 1 to 1023.

When you clear the monitor sessions, follow these syntax guidelines:

- The **no monitor session** *session-number* command entered with no other parameters clears the session *session-number*.
- *session-range* is *first-session-number-last-session-number*.



**Note** When you enter the **no monitor session range** command, do not enter spaces before or after the dash. If you enter multiple ranges, do not enter spaces before or after the commas.

## Examples

This example shows how to configure an ERSPAN source session number and enter the ERSPAN source session configuration mode for the session:

```
Router(config)# monitor session 55 type erspan-source
Router(config-mon-erspan-src)#
```

This example shows how to configure an ERSPAN destination session number and enter the ERSPAN destination session configuration mode for the session:

```
Router(config)# monitor session 55 type erspan-destination
Router(config-mon-erspan-dst)#
```

This example shows how to associate the ERSPAN destination session number with the destination ports:

```
Router(config-mon-erspan-dst) destination interface fastethernet 1/2 , 2/3
```

This example shows how to enter the ERSPAN destination session source configuration:

```
Router(config-mon-erspan-dst)# source
Router(config-mon-erspan-dst-src)#
```

This example shows how to enter the ERSPAN destination session source configuration mode:

```
Router(config-mon-erspan-dst)# source
Router(config-mon-erspan-dst-src)#
```

This example shows how to configure multiple sources for a session:

```
Router(config-mon-erspan-src)# source interface fastethernet 5/15 , 7/3 rx
Router(config-mon-erspan-src)# source interface gigabitethernet 1/2 tx
Router(config-mon-erspan-src)# source interface port-channel 102
Router(config-mon-erspan-src)# source filter vlan 2 - 3
Router(config-mon-erspan-src)#
```

This example shows how to enter the ERSPAN source session destination configuration mode:

```
Router(config-mon-erspan-src)# destination
Router(config-mon-erspan-src-dst)#
```

This example shows how to configure the ID number that is used by the source and destination sessions to identify the ERSPAN traffic:

```
Router(config-mon-erspan-src-dst)# erspan-id 1005
Router(config-mon-erspan-src-dst)#
```

---

**Related Commands**

Command	Description
<a href="#">show monitor session</a>	Displays information about the ERSPAN, SPAN, and RSPAN sessions.

# mpls l2transport route

To enable routing of Layer 2 packets over MPLS, use the **mpls l2transport route** command. To disable routing over MPLS, use the **no** form of this command.

**mpls l2transport route** *destination vc-id*

**no mpls l2transport route** *destination vc-id*

Syntax Description	
<i>destination</i>	IP address of the router to which the virtual circuit is destined.
<i>vc-id</i>	Virtual-circuit identification to a router.

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

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **mpls l2transport route** command enables the virtual connection used to route the VLAN packets. The types of virtual connections used are as follows:

- VC Type 4—Allows all the traffic in a VLAN to use a single VC across the MPLS network.
- VC Type 5—Allows all traffic on a port to share a single VC across the MPLS network.

During the VC setup, VC type 5 is advertised. If the peer advertises VC type 4, the VC type is changed to type 4 and the VC is restarted. Note that the change only happens from type 5 to type 4 and never from type 4 to type 5.

An MPLS VLAN virtual circuit in Layer 2 runs across an MPLS cloud to connect the VLAN interfaces on two PE routers.

Use the **mpls l2transport route** command on the VLAN interface of each PE router to route the VLAN packets in Layer 2 across the MPLS cloud to the VLAN interface of the other PE router. Specify the IP address of the other PE router for the destination parameter. Do not specify the IP address of the router from which you are issuing the command.

You can choose any value for the virtual-connection ID. However, the virtual-circuit ID must be unique to the virtual connection. In large networks, you may need to track the virtual-connection ID assignments to ensure that a virtual-connection ID does not get assigned twice.

The routed virtual connections are supported on the main interfaces, not subinterfaces.

The virtual-circuit ID must be unique to each virtual connection.

## ■ mpls l2transport route

---

**Examples**

This example shows how to enable routing of Layer 2 packets over MPLS:

```
Router(config-if)# mpls l2transport route 192.16.0.1
Router(config-if)#
```

---

**Related Commands**

Command	Description
<a href="#">show mpls l2transport vc</a>	Displays the state of virtual circuits on a router.

# mpls load-balance per-label

To enable the load balancing for the tag-to-tag traffic, use the **mpls load-balance per-label** command. To return to the default settings, use the **no** form of this command.

**mpls load-balance per-label**

**no mpls load-balance per-label**

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

**Defaults** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** When you enable load balancing for the tag-to-tag traffic, the traffic is balanced based on the incoming label (per prefix) among MPLS interfaces. Each MPLS interface supports an equal number of incoming labels.

You can use the **show mpls ttfib** command to display the incoming label (indicated by an asterisk) that is included in the load balancer.

**Examples** This example shows how to enable the load balancing for the tag-to-tag traffic:

```
Router(config)# mpls load-balance per-label
Router(config)#
```

This example shows how to disable the load balancing for the tag-to-tag traffic:

```
Router(config)# no mpls load-balance per-label
Router(config)#
```

Related Commands	Command	Description
	<b>show mpls ttfib</b>	Displays information about the MPLS TTFIB table.

# mpls ttl-dec

To specify standard MPLS tagging, use the **mpls ttl-dec** command. To return to the default settings, use the **no** form of this command.

**mpls ttl-dec**

**no mpls ttl-dec**

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

**Defaults** Optimized MPLS tagging (**no mpls ttl-dec**).

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** MPLS tagging has been optimized to allow the rewriting of the original packet's IP ToS and TTL values before the MPLS label is pushed onto the packet header. This change can result in a slightly lower performance for certain types of traffic. If the packet's original ToS/TTL values are not significant, you enter the **mpls ttl-dec** command for standard MPLS tagging.

**Examples** This example shows how to configure the Catalyst 6500 series switch to use standard MPLS tagging behavior:

```
Router(config)# mpls ttl-dec
Router(config)#
```

This example shows how to configure the Catalyst 6500 series switch to use optimized MPLS tagging behavior:

```
Router(config)# no mpls ttl-dec
Router(config)#
```

Related Commands	Command	Description
	<a href="#">mpls l2transport route</a>	Enables routing of Layer 2 packets over MPLS.

# mtu

To adjust the maximum packet size or MTU size, use the **mtu** command. To return to the default settings, use the **no** form of this command.

**mtu** *bytes*

**no mtu**

Syntax Description	<i>bytes</i>
	Byte size; valid values are from 64 to 9216 for SVI ports, from 1500 to 9170 for the GE-WAN+ ports, and from 1500 to 9216 for all other ports.

## Defaults

Table 2-27 lists the default MTU values if you disable the jumbo frames.

**Table 2-27 Default MTU Values**

Media Type	Default MTU (bytes)
Ethernet	1500
Serial	1500
Token Ring	4464
ATM	4470
FDDI	4470
HSSI (HSA)	4470

If you enable the jumbo frames, the default is 64 for the SVI ports and 9216 for all the other ports. The jumbo frames are disabled by default.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

For switch ports, only one larger-than-default MTU value is allowed globally. For Layer 3 ports, including router ports and VLANs, you can configure nondefault MTU values on a per-interface basis.

For a complete list of modules that do not support jumbo frames, refer to the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*.

Changing the MTU value with the **mtu** command can affect values for the protocol-specific versions of the command (for example, the **ip mtu** command). If the values that are specified with the **ip mtu** command are the same as the value that is specified with the **mtu** command, and you change the value for the **mtu** command, the **ip mtu** value automatically matches the new **mtu** command value. However, changing the values for the **ip mtu** command has no effect on the value for the **mtu** command.

---

**Examples**

This example shows how to specify an MTU of 1800 bytes:

```
Router(config)# interface fastethernet 5/1  
Router(config-if)# mtu 1800
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ip mtu</b>	Sets the MTU size of IP packets sent on an interface.

---

## name (MST configuration submode)

To set the name of an MST region, use the **name** command. To return to the default name, use the **no** form of this command.

**name** *name*

**no name** *name*

Syntax Description	<i>name</i>
	Name to give the MST region. It can be any string with a maximum length of 32 characters.

Defaults	Empty string
----------	--------------

Command Modes	MST configuration submode
---------------	---------------------------

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Usage Guidelines	Two or more Catalyst 6500 series switches with the same VLAN mapping and configuration version number are considered to be in different MST regions if the region names are different.
------------------	--



### Caution

Be careful when using the **name** command to set the name of an MST region. If you make a mistake, you can put the Catalyst 6500 series switch in a different region. The configuration name is a case-sensitive parameter.

Examples	This example shows how to name a region:
----------	--

```
Router(config-mst)# name Cisco
Router(config-mst)#
```

■ name (MST configuration submode)

Related Commands	Command	Description
	<b>instance</b>	Maps a VLAN or a set of VLANs to an MST instance.
	<b>revision</b>	Sets the revision number for the MST configuration.
	<b>show</b>	Verifies the MST configuration.
	<b>show spanning-tree mst</b>	Displays the information about the MST protocol.
	<b>spanning-tree mst configuration</b>	Enters MST-configuration submode.

# neighbor

To specify the type of tunnel signaling and encapsulation mechanism for each peer, use the **neighbor** command. To disable a split horizon, use the **no** form of this command.

```
neighbor remote-router-id {encapsulation encapsulation-type} | {pw-class pw-name}
[no-split-horizon]
```

```
no neighbor remote-router-id
```

Syntax Description	
<i>remote-router-id</i>	Remote peering router identification.
<b>encapsulation</b> <i>encapsulation</i>	Specifies the tunnel encapsulation type; valid values are <b>l2tpv3</b> and <b>mpls</b> .
<b>pw-class</b> <i>pw-name</i>	Specifies the pseudo-wire property to be used to set up the emulated VC.
<b>no-split-horizon</b>	(Optional) Disables the Layer 2 split horizon in the data path.

**Defaults** Split horizon is enabled.

**Command Modes** Layer 2 VFI manual configuration submode

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

To avoid looping, you should not disable a split horizon in a fully meshed Virtual PVLAN service (VPLS) network.

**Examples** This example shows how to specify the tunnel encapsulation type:

```
Router(config-vfi)# neighbor 333 encapsulation mpls
Router(config-vfi)#
```

This example shows how to disable the Layer 2 split horizon in the data path:

```
Router(config-vfi)# neighbor 333 no-split-horizon
Router(config-vfi)#
```

# net

To configure an IS-IS NET for the routing process, use the **net** command. To remove a NET, use the **no** form of this command.

```
net net1 {alt net2}
```

```
no net net
```

## Syntax Description

<i>net1</i>	NET NSAP name or address for the IS-IS routing process on the PISA in the primary slot; see the “Usage Guidelines” section for additional information.
<b>alt</b> <i>net2</i>	Specifies the NET name or address for the IS-IS routing process on the PISA in the alternate slot; see the “Usage Guidelines” section for additional information.
<i>net</i>	NET NSAP name or address to be removed.

## Defaults

The defaults are as follows:

- No NET is configured.
- IS-IS process is disabled.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

A NET is an NSAP where the last byte is always the n-selector and is always zero. A NET can be from 8 to 20 bytes.

Under most circumstances, you should configure one NET only.

When entering the *net*, use these guidelines:

- In a 3-slot chassis, slot 1 is the primary slot and slot 2 is the alternate slot.
- In a 6-slot chassis, slot 5 is the primary slot and slot 6 is the alternate slot.
- In a 9-slot chassis, slot 5 is the primary slot and slot 6 is the alternate slot.
- In a 13-slot chassis, slot 7 is the primary slot and slot 8 is the alternate slot.

If you are using IS-IS to perform IP routing only (no connectionless network service routing is enabled), you must configure a NET to define the router ID and area ID.

Multiple NETs per router are allowed with a maximum of three NETs. In rare circumstances, you can configure two or three NETs. In such a case, the area this router is in will have three area addresses and only one area.

Multiple NETs can be temporarily useful for network reconfiguration where multiple areas are merged, or where one area is split into more areas. Multiple area addresses enable you to renumber an area individually as needed.

### Examples

This example shows how to configure a router with system ID 0000.0c11.1110 and area ID 47.0004.004d.0001:

```
router isis Pieinthesky
 net 47100041004d100041000410c4414444100
```

This example shows three IS-IS routing processes with three areas that are configured. Each area has a unique identifier, but the system ID is the same for all areas.

```
clns routing

111

interface Tunnel559
 ip address 40101015 5551555155510
 ip router isis BB
 clns router isis BB

interface Ethernet4
 ip address 40141415 5551555155510
 ip router isis A3553-04
 clns router isis A3553-04
!
interface Ethernet5
 ip address 40151515 5551555155510
 ip router isis A3553-05
 clns router isis A3553-05

111

router isis BB                                ! Defaults to "is-type level-4-5"
 net 4915555100001000010005100
!
router isis A3553-04
 net 491055310004100001000010005100
 is-type level-4
!
router isis A3553-05
 net 491055310005100001000010005100
 is-type level-4
```

### Related Commands

Command	Description
<b>is-type</b>	Configures the routing level for an instance of the IS-IS routing process.
<b>router isis</b>	Enables the IS-IS routing protocol and specifies an IS-IS process.

# nsf

To enable and configure Cisco NSF, use the **nsf** command. To disable NSF, use the **no** form of this command.

**nsf [enforce global]**

**nsf** [{**cisco** | **ietf**} | {**interface** {**wait** *seconds*}} | {**interval** *minutes*} | {**t3** [**adjacency** | {**manual** *seconds*}}}]

**no nsf**

Syntax Description	
<b>enforce global</b>	(Optional) Cancels OSPF NSF restart when non-NSF-aware neighbors are detected.
<b>cisco</b>	(Optional) Specifies the Cisco proprietary IS-IS NSF method of checkpointing if the active RP fails over.
<b>ietf</b>	(Optional) Specifies the IETF IS-IS NSF method of protocol modification if the active RP fails over.
<b>interface wait</b> <i>seconds</i>	(Optional) Specifies how long to wait for an interface to come up after failover before it proceeds with the Cisco NSF process; valid values are from 1 to 60 seconds.
<b>interval</b> <i>minutes</i>	(Optional) Specifies how long to wait after a route processor stabilizes before restarting; valid values are from 0 to 1440 minutes.
<b>t3 adjacency</b>	(Optional) Specifies that the time that IETF NSF waits for the LSP database to synchronize is determined by the adjacency holdtime advertised to the neighbors of the specified RP before switchover.
<b>t3 manual</b> <i>seconds</i>	(Optional) Specifies the time to wait after the NSF database synchronizes before informing other nodes to remove the restarting node from consideration as a transit; valid values are from 5 to 3600 seconds.

## Defaults

The default settings are as follows:

- NSF is disabled.
- **enforce global**—Enabled.
- **interval** *minutes*—5 minutes.
- **interface wait** *seconds*—10 seconds.
- **t3 manual** *seconds*—30 seconds.

## Command Modes

Router configuration IS-IS

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

The **nsf interface wait** command can be used if Cisco proprietary IS-IS NSF is configured or if the Internet Engineering Task Force (IETF) IS-IS NSF is enabled using the **nsf t3 manual** command. You can use this command if an interface is slow to come up.

**Note**

Cisco NSF is required only if the Catalyst 6500 series switch is expected to perform Cisco NSF during a restart. If the Catalyst 6500 series switch is expected to cooperate with a neighbor that is doing a Cisco NSF restart only, the switch must be NSF capable by default (running a version of code that supports Cisco NSF), but Cisco NSF does not have to be configured on the switch.

The **nsf** commands are a subset of the **router** command and affects all the interfaces that are covered by the designated process. Cisco NSF supports the BGP, OSPF, IS-IS, and EIGRP protocols. The configuration commands that enable NSF processing are as follows:

- **nsf** under the **router ospf** command
- **nsf ietf** under the **router isis** command
- **bgp graceful-restart** under the **router bgp** command

These commands must be issued as part of the router's running configuration. During the restart, these commands are restored to activate the NSF processing.

The `[[{cisco | ietf} | {interface {wait seconds}} | {interval minutes} | {t3 [adjacency | {manual seconds}]]]` keywords and arguments apply to IS-IS only.

The `{enforce global}` keywords apply to OSPF only.

**BGP NSF Guidelines**

BGP support in NSF requires that neighbor networking devices be NSF-aware devices; that is, they must have the graceful restart capability and advertise that capability in the OPEN message during session establishment. If an NSF-capable router discovers that a particular BGP neighbor does not have the graceful restart capability enabled, it will not establish an NSF-capable session with that neighbor. All other neighbors that have a graceful restart capability will continue to have NSF-capable sessions with this NSF-capable networking device. Enter the **bgp graceful-restart** router configuration command to enable the graceful restart capability. Refer to the *Cisco IOS Release 12.2 Command Reference* for more information.

**EIRGP NSF Guidelines**

A router may be an NSF-aware router but may not be participating in helping out the NSF restarting neighbor because it is coming up from a cold start.

**IS-IS NSF Guidelines**

If you configure IETF on the networking device, but neighbor routers are not IETF-compatible, NSF will abort after the switchover.

Use these two keywords when configuring IS-IS NSF:

- **ietf**—Internet Engineering Task Force IS-IS—After a supervisor engine switchover, the NSF-capable router sends the IS-IS NSF restart requests to the neighboring NSF-aware devices.
- **cisco**—Cisco IS-IS. Full adjacency and LSP information is saved (checkpointed) to the standby supervisor engine. After a switchover, the newly active supervisor engine maintains its adjacencies using the checkpointed data to quickly rebuild its routing tables.

## OSPF NSF Guidelines

OSPF NSF requires that all neighbor networking devices be NSF-aware devices. If an NSF-capable router discovers that it has non-NSF aware neighbors on a particular network segment, it will disable the NSF capabilities for that segment. The other network segments that are composed entirely of NSF-capable or NSF-aware routers will continue to provide NSF capabilities.

OSPF NSF supports NSF/SSO for IPv4 traffic only. OSPFv3 is not supported with NSF/SSO. Only OSPFv2 is supported with NSF/SSO.

### Examples

This example shows how to enable NSF for all OSPF-process interfaces:

```
Router(config)# router ospf 109
Router(config-router)# nsf
Router(config-router)#
```

This example shows how to disable NSF for all OSPF-process interfaces:

```
Router(config)# router ospf 109
Router(config-router)# no nsf
Router(config-router)#
```

### Related Commands

Command	Description
<b>router</b>	Enables a routing process.

# pagp learn-method

To learn the input interface of the incoming packets, use the **pagp learn-method** command. To return to the default settings, use the **no** form of this command.

```
pagp learn-method { aggregation-port | physical-port }
```

```
no pagp learn-method
```

Syntax Description	
<b>aggregation-port</b>	Specifies how to learn the address on the port channel.
<b>physical-port</b>	Specifies how to learn the address on the physical port within the bundle.

Defaults	
	<b>aggregation-port</b> method

Command Modes	
	Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Examples	
	This example shows how to set the learning method to learn the address on the physical port within the bundle:

```
Router(config-if)# pagp learn-method physical-port
Router(config-if)#
```

This example shows how to set the learning method to learn the address on the port channel within the bundle:

```
Router(config-if)# pagp learn-method
Router(config-if)#
```

Related Commands	Command	Description
	<a href="#">show pagp</a>	Displays port-channel information.

## pagp port-priority

To select a port in hot standby mode, use the **pagp port-priority** command. To return to the default settings, use the **no** form of this command.

**pagp port-priority** *priority*

**no pagp port-priority**

<b>Syntax Description</b>	<i>priority</i> Priority number; valid values are from 1 to 255.
---------------------------	--

<b>Defaults</b>	<i>priority</i> is <b>128</b> .
-----------------	---------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	The higher the priority means the better the chances are that the port will be selected in the hot standby mode.
-------------------------	--

<b>Examples</b>	This example shows how to set the port priority:
-----------------	--

```
Router(config-if)# pagp port-priority 45
Router(config-if)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">pagp learn-method</a>	Learns the input interface of the incoming packets.
	<a href="#">show pagp</a>	Displays port-channel information.

# platform ip features sequential

To enable IP precedence-based or DSCP-based egress QoS filtering to use any IP precedence or DSCP policing or marking changes made by ingress PFC QoS, use the **platform ip features sequential** command. To return to the default settings, use the **no** form of this command.

**platform ip features sequential** [**access-group** {*ip-acl-name* | *ip-acl-number*}]

**no platform ip features sequential** [**access-group** {*ip-acl-name* | *ip-acl-number*}]

## Syntax Description

<b>access-group</b> <i>ip-acl-name</i>	(Optional) Specifies the name of the ACL that is used to specify the match criteria for the recirculation packets.
<b>access-group</b> <i>ip-acl-number</i>	(Optional) Specifies the number of the ACL that is used to specify the match criteria for the recirculation packets; valid values are from 1 to 199 and from 1300 to 2699.

## Defaults

IP precedence-based or DSCP-based egress QoS filtering uses received IP precedence or DSCP values and does not use any IP precedence or DSCP changes made by ingress QoS as the result of policing or marking.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

The enhanced egress-QoS filtering enables the IP precedence-based or DSCP-based egress-QoS filtering to use any IP precedence or DSCP policing or marking changes made by ingress QoS.

The nonenhanced egress-QoS filtering behavior is the normal Catalyst 6500 series switch behavior when QoS is applied in the hardware.

The PFC3 provides egress PFC QoS only for Layer 3-switched and routed traffic on egress Layer 3 interfaces (either LAN ports configured as Layer 3 interfaces or VLAN interfaces).

You configure enhanced egress QoS filtering on ingress Layer 3 interfaces (either LAN ports configured as Layer 3 interfaces or VLAN interfaces).

To enable enhanced egress QoS filtering only for the traffic filtered by a specific standard, extended named, or extended numbered IP ACL, enter the IP ACL name or number.

If you do not enter an IP ACL name or number, enhanced egress QoS filtering is enabled for all IP ingress IP traffic on the interface.

**Note**

When you configure enhanced egress-QoS filtering, the PFC3A processes traffic to apply ingress PFC QoS. The PFC3A applies ingress-QoS filtering and Catalyst 6500 series switch hardware ingress QoS. The PFC3A incorrectly applies any egress-QoS filtering and Catalyst 6500 series switch hardware egress QoS that is configured on the ingress interface.

**Note**

If you configure enhanced egress-QoS filtering on an interface that uses Layer 2 features to match the IP precedence or DSCP as modified by ingress-QoS marking, the packets are redirected or dropped and prevented from being processed by egress QoS.

**Note**

If you enable enhanced egress-QoS filtering, the hardware acceleration of NetFlow-based features such as reflexive ACL, NAT, and TCP intercept are disabled.

To verify configuration, use the **show running-config interface** command.

**Examples**

This example shows how to enable enhanced egress-QoS filtering:

```
Router(config-if)# platform ip features sequential
Router(config-if)#
```

This example shows how to disable enhanced egress-QoS filtering:

```
Router(config-if)# no platform ip features sequential
Router(config-if)#
```

**Related Commands**

Command	Description
<b>show running-config interface</b>	Displays the contents of the currently running configuration file.

# platform ipv6 acl icmp optimize neighbor-discovery

To optimize TCAM support for IPv6 ACLs, use the **platform ipv6 acl icmp optimize neighbor-discovery** command. To disable optimization of TCAM support for IPv6 ACLs, use the **no** form of this command.

**platform ipv6 acl icmp optimize neighbor-discovery**

**no platform ipv6 acl icmp optimize neighbor-discovery**

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

**Defaults** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines



**Note** Use this command under the direction of the Cisco TAC only.

When you enable optimization of the TCAM support for IPv6 ACLs, the global ICMPv6 neighbor-discovery ACL at the top of the TCAM is programmed to permit all ICMPv6 neighbor-discovery packets. Enabling optimization prevents the addition of ICMPv6 ACEs at the end of every IPv6 security ACL, reducing the number of TCAM resources being used. Enabling this command reprograms IPv6 ACLs on all interfaces.



**Note** The ICMPv6 neighbor-discovery ACL at the top of the TCAM takes precedence over security ACLs for ICMP neighbor-discovery packets that you have configured, but has no effect if you have a bridge/deny that overlaps with the global ICMP ACL.

**platform ipv6 acl icmp optimize neighbor-discovery****Examples**

This example shows how to optimize TCAM support for IPv6 ACLs:

```
Router(config)# platform ipv6 acl icmp optimize neighbor-discovery  
Router(config)#
```

This example shows how to disable optimization of TCAM support for IPv6 ACLs:

```
Router(config)# no platform ipv6 acl icmp optimize neighbor-discovery  
Router(config)#
```

# platform scp retry interval

To enable SCP fast retry and set the fast-retry interval, use the **platform scp retry interval** command. To disable SCP fast retry, use the **no** form of this command.

**platform scp retry interval** *timeout-value*

**no platform scp retry interval**

<b>Syntax Description</b>	<i>timeout-value</i> Fast retry interval; valid values are from 200 to 2000 milliseconds.
---------------------------	---

<b>Defaults</b>	<b>2000</b> milliseconds
-----------------	--------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines



**Note** Use this command under the direction of the Cisco TAC only.

## Examples

This example shows how to enable SCP fast retry and set the fast-retry interval:

```
Router(config)# platform scp retry interval 600
Router(config)#
```

# platform vfi dot1q-transparency

To enable 802.1Q transparency mode, use the **platform vfi dot1q-transparency** command. To disable 802.1Q transparency, use the **no** form of this command.

**platform vfi dot1q-transparency**

**no platform vfi dot1q-transparency**

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

**Defaults** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command is supported on OSM modules only.

The 802.1Q transparency allows a service provider to modify the MPLS EXP bits for core-based QoS policies while leaving any VPLS customer 802.1p bits unchanged.

The dot1q Transparency for EoMPLS feature causes the VLAN-applied policy to affect only the IGP label (for core QoS) and leaves the VC label EXP bits equal to the 802.1p bits. On the egress PE, the 802.1p bits are still rewritten based on the received VC EXP bits, however, because the EXP bits now match the ingress 802.1p bits, a VPLS customer's 802.1p bits do not change.

Global configuration applies to all virtual forwarding instance (VFI) and switched virtual interface (SVI) EoMPLS VCs configured on the Cisco 7600 series routers.

Interoperability requires applying the Dot1q Transparency for EoMPLS feature to all participating PE routers.

**Examples** This example shows how to enable 802.1Q transparency:

```
Router (config)# platform vfi dot1q-transparency
Router (config)#
```

This example shows how to disable 802.1Q transparency:

```
Router (config)# no platform vfi dot1q-transparency
Router (config)#
```

# police (policy map)

To create a per-interface policer and configure the policy-map class to use it, use the **police** command. To delete the per-interface policer from the policy-map class, use the **no** form of this command.

```
police {bits-per-second [normal-burst-bytes] [maximum-burst-bytes] [pir peak-rate-bps]} |
[conform-action action] [exceed-action action] [violate-action action]
```

```
no police {bits-per-second [normal-burst-bytes] [extended-burst-bytes] [pir peak-rate-bps]} |
[conform-action action] [exceed-action action] [violate-action action]
```

Syntax Description		
<i>bits-per-second</i>		CIR bits per second; valid values are from 32000 to 2 Gbps bits per second.
<i>normal-burst-bytes</i>		(Optional) CIR token-bucket size; valid values are from 1000 to 512000000 bytes.
<i>maximum-burst-bytes</i>		(Optional) PIR token-bucket size; valid values are from 1000 to 32000000 bytes.
<b>pir</b> <i>peak-rate-bps</i>		(Optional) Sets the PIR peak rate; valid values are from 32000 to 2 Gbps bits per second.
<b>conform-action</b> <i>action</i>		(Optional) Specifies the action to be taken if the <i>bits-per-second</i> rate has not been exceeded; see the “Usage Guidelines” section for valid values.
<b>exceed-action</b> <i>action</i>		(Optional) Specifies the action to be taken when the <i>bits-per-second</i> rate has been exceeded; see the “Usage Guidelines” section for valid values.
<b>violate-action</b> <i>action</i>		(Optional) Specifies the action to be taken when the <i>bits-per-second</i> rate is greater than the <i>maximum-burst-bytes</i> rate; see the “Usage Guidelines” section for valid values.

## Defaults

The defaults are as follows:

- *maximum-burst-bytes* is equal to *normal-burst-bytes*.
- **conform-action** is **transmit**.
- **exceed-action** is **drop**.
- **violate-action** is equal to the **exceed-action**.
- **pir** *peak-rate-bps* is equal to the *normal-burst-bytes* rate.

## Command Modes

Policy-map subcommand

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

On the Supervisor Engine 32 PISA, the **police** command is supported in software.

Named aggregate policers and microflow policers are not supported on the Supervisor Engine 32 PISA.

The *normal-burst-bytes* argument sets the CIR token bucket size.

The *maximum-burst-bytes* argument sets the PIR token bucket size (not supported with the **flow** keyword). You must set the *maximum-burst-bytes* argument to be equal to the *normal-burst-bytes* setting.

The **pir** *peak-rate-bps* corresponds to the *extended-burst-bytes*.

The valid values for *action* are as follows:

- **drop**—Drops packets that do not exceed the *bits-per-second* rate.
- **policed-dscp-transmit**—Causes all the out-of-profile traffic to be marked down as specified in the markdown map.
- **set-dscp-transmit** {*dscp-value* | *dscp-bit-pattern* | **default** | **ef**}—Marks the matched traffic with a new DSCP value where the valid values are as follows:
  - *dscp-value*—Specifies a DSCP value; valid values are from 0 to 63.
  - *dscp-bit-pattern*—Specifies a DSCP bit pattern; valid values are listed in [Table 2-28](#).
  - **default**—Matches packets with default dscp (000000).
  - **ef**—Matches packets with EF dscp (101110).

**Table 2-28 Valid dscp-bit-pattern Values**

Keyword	Definition
<b>af11</b>	Matches packets with AF11 dscp (001010).
<b>af12</b>	Matches packets with AF12 dscp (001100).
<b>af13</b>	Matches packets with AF13 dscp (001110).
<b>af21</b>	Matches packets with AF21 dscp (010010).
<b>af22</b>	Matches packets with AF22 dscp (010100).
<b>af23</b>	Matches packets with AF23 dscp (010110).
<b>af31</b>	Matches packets with AF31 dscp (011010).
<b>af32</b>	Matches packets with AF32 dscp (011100).
<b>af33</b>	Matches packets with AF33 dscp (011110).
<b>af41</b>	Matches packets with AF41 dscp (100010).
<b>af42</b>	Matches packets with AF42 dscp (100100).
<b>af43</b>	Matches packets with AF43 dscp (100110).
<b>cs1</b>	Matches packets with CS1 (precedence 1) dscp (001000).
<b>cs2</b>	Matches packets with CS2 (precedence 2) dscp (010000).
<b>cs3</b>	Matches packets with CS3 (precedence 3) dscp (011000).
<b>cs4</b>	Matches packets with CS4 (precedence 4) dscp (100000).
<b>cs5</b>	Matches packets with CS5 (precedence 5) dscp (101000).
<b>cs6</b>	Matches packets with CS6 (precedence 6) dscp (110000).
<b>cs7</b>	Matches packets with CS7 (precedence 7) dscp (111000).

- **set-mpls-exp-imposition-transmit** *new-mpls-exp*—Rewrites the MPLS experimental bits on imposed label entries and transmits. The *new-mpls-exp* argument specifies the value used to set the MPLS EXP bits that are defined by the policy map; valid values for *new-mpls-exp* are from 0 to 7.
- **set-mpls-exp-topmost-transmit**—Rewrites the MPLS experimental bits on the topmost label entries and transmits. The *new-mpls-exp* argument specifies the value used to set the MPLS EXP bits that are defined by the policy map; valid values for *new-mpls-exp* are from 0 to 7.
- **set-prec-transmit** *new-precedence*—Marks the matched traffic with a new IP-precedence value and transmits; valid values for *new-precedence* are from 0 to 7.
- **transmit**—Transmits the packets that do not exceed the *bits-per-second* rate.

## Examples

This example shows how to create a policy map named max-pol-ipp5 that uses the class map named ipp5, which is configured to trust received IP-precedence values and is configured with a maximum-capacity aggregate policer:

```
Router# configure terminal
Enter configuration commands, one per line! End with CNTL/]]
Router(config)# policy-map max-pol-ipp5
Router(config-pmap)# class ipp5
Router(config-pmap-c)# trust ip-precedence
Router(config-pmap-c)# police 2000000000 2000000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)#
```

## Related Commands

Command	Description
<a href="#">class-map</a>	Accesses the QoS class map configuration mode to configure QoS class maps.
<a href="#">service-policy</a>	Attaches a policy map to an interface.
<a href="#">show class-map</a>	Displays class-map information.
<a href="#">show policy-map</a>	Displays information about the policy map.
<a href="#">show policy-map interface</a>	Displays the statistics and the configurations of the input and output policies that are attached to an interface.

## police rate

To configure traffic policing for traffic that is destined for the control plane, use the **police rate** command. To remove traffic policing from the configuration, use the **no** form of this command.

**police rate** *units* **pps** [**burst** *burst-in-packets* **packets**] [**peak-rate** *peak-rate-in-pps* **pps**] [**peak-burst** *peak-burst-in-packets* **packets**]

**police rate** *units* **bps** [**burst** *burst-in-bytes* **bytes**] [**peak-rate** *peak-rate-in-bps* **bps**] [**peak-burst** *peak-burst-in-bytes* **bytes**]

**police rate percent** *percentage* [**burst** *ms* **ms**] [**peak-rate percent** *percentage*] [**peak-burst** *ms* **ms**]

**no police rate** *units* **pps** [**burst** *burst-in-packets* **packets**] [**peak-rate** *peak-rate-in-pps* **pps**] [**peak-burst** *peak-burst-in-packets* **packets**]

**no police rate** *units* **bps** [**burst** *burst-in-bytes* **bytes**] [**peak-rate** *peak-rate-in-bps* **bps**] [**peak-burst** *peak-burst-in-bytes* **bytes**]

**no police rate percent** *percentage* [**burst** *ms* **ms**] [**peak-rate percent** *percentage*] [**peak-burst** *ms* **ms**]

### Syntax Description

<i>units</i>	Police rate; see the “Usage Guidelines” section for valid values.
<b>pps</b>	Specifies that the rate at which traffic is policed is in packets per second.
<b>burst</b> <i>burst-in-packets</i> <b>packets</b>	(Optional) Specifies the burst rate that is used for policing traffic; valid values are from 1 to 512000 packets.
<b>peak-rate</b> <i>peak-rate-in-pps</i> <b>pps</b>	(Optional) Specifies the PIR that is used for policing traffic; valid values are from from 1 to 512000 packets.
<b>peak-burst</b> <i>peak-burst-in-packets</i> <b>packets</b>	(Optional) Specifies the peak-burst value that is used for policing traffic; valid values are from 1 to 512000 packets.
<b>bps</b>	Specifies that the rate at which traffic is policed is in bits per second.
<b>burst</b> <i>burst-in-bytes</i> <b>bytes</b>	(Optional) Specifies the burst rate that is used for policing traffic; valid values are from 1000 to 512000000 bits.
<b>peak-rate</b> <i>peak-rate-in-bps</i> <b>bps</b>	(Optional) Specifies the peak burst value that is used for the peak rate; valid values are from 1000 to 512000000 bits.
<b>peak-burst</b> <i>peak-burst-in-bytes</i> <b>bytes</b>	(Optional) Specifies the peak burst value that is used for policing traffic; valid values are from 1000 to 512000000 bits.
<b>percent</b> <i>percentage</i>	(Optional) Specifies the percentage of interface bandwidth that is used to determine the rate at which traffic is policed; valid values are from 1 to 100.
<b>burst</b> <i>ms</i> <b>ms</b>	(Optional) Specifies the burst rate that is used for policing traffic; valid values are from 1 to 2000 milliseconds.
<b>peak-rate percent</b> <i>percentage</i>	(Optional) Specifies the percentage of the interface bandwidth that is used to determine the PIR; valid values are from 1 to 100.
<b>peak-burst</b> <i>ms</i> <b>ms</b>	(Optional) Specifies the peak burst rate that is used for policing traffic; valid values are from 1 to 2000 milliseconds.

**Defaults** Disabled

**Command Modes** Policy-map class configuration

Release	Modification
12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The valid values for *units* are as follows:

- If the police rate is specified in pps, the valid values are from 1 to 2000000 pps.
- If the police rate is specified in bps, the valid values are from 8,000 to 10,000,000,000 bps.

pps is used to calculate the PIR *peak-rate-in-pps*.

Use the **police rate** command to limit traffic that is destined for the control plane on the basis of packets per second (pps), bytes per seconds (bps), or a percentage of interface bandwidth.

If the **police rate** command is entered, but the rate is not specified, traffic that is destined for the control plane will be policed on the basis of bps.

**Examples** This example shows how to configure policing on a class to limit traffic to an average rate of 1500000 pps:

```
Router(config)# class-map telnet-class
Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map control-plane-policy
Router(config-pmap)# class telnet-class
Router(config-pmap-c)# police rate 1500000 pps bc 500000 packets
Router(config-pmap-c)# exit
```

Related Commands	Command	Description
	<a href="#">policy-map</a>	Accesses QoS policy-map configuration mode to configure the QoS policy map.
	<a href="#">show policy-map</a>	Displays information about the policy map.

# policy-map

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

**policy-map** *policy-map-name*

**no policy-map** *policy-map-name*

## Syntax Description

*policy-map-name* Policy map name. See the “Usage Guidelines” section for descriptions of the **policy-map** subcommands.

## Defaults

The defaults are as follows:

- *extended-burst-bytes* is equal to *burst-bytes*.
- **conform-action** is transmit.
- **exceed-action** is drop.
- **violate-action** is equal to the **exceed-action**.
- **pir** *peak-rate-bps* is equal to the normal (**cir**) rate.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

In QoS policy-map configuration mode, these configuration commands are available:

- **exit** exits QoS class-map configuration mode.
- **no** removes a previously defined policy map.
- **class** *class-map* [*name*] accesses QoS class-map configuration mode to specify a previously created class map to be included in the policy map or to create a class map (see the **class-map** command for additional information).
- **class** {*class-name* | **class-default**} accesses the class configuration mode to specify the name of the class whose policy you want to create or change (see the **class (policy-map)** command for additional information).
- **police** [**aggregate** *name*] subcommand defines a microflow or aggregate policer (see the **police (policy map)** command for additional information) and provides the following syntaxes:
  - **police** {**aggregate** *name*}
  - **police flow** {*bits-per-second* [*normal-burst-bytes*] [*maximum-burst-bytes*] [**pir** *peak-rate-bps*]} | [**conform-action** *action*] [**exceed-action** *action*] [**violate-action** *action*]

- **police flow mask** {**dest-only** | **full-flow** | **src-only**} {*bits-per-second* [*normal-burst-bytes*] [*maximum-burst-bytes*]} [**conform-action** *action*] [**exceed-action** *action*]
- **trust** {**cos** | **dscp** | **ip-precedence**} sets the specified class trust values. Trust values that are set in this command supersede trust values that are set on specific interfaces.

Table 2-29 describes the **class** syntax.

**Table 2-29 class Syntax Description**

Subcommand	Description
<b>exit</b>	(Optional) Exits from QoS class action configuration mode.
<b>police</b>	(Optional) Specifies flow policing; see the <b>police (policy map)</b> command for additional information.
<b>trust state</b>	(Optional) Configures the policy map class trust state. Trust states are <b>cos</b> , <b>dscp</b> , and <b>ip-precedence</b> .
<b>cos</b>	(Optional) Sets the internal DSCP value from a received or interface CoS.
<b>dscp</b>	(Optional) Sets QoS to use the received DSCP value.
<b>ip-precedence</b>	(Optional) Sets the DSCP value from the received IP precedence.

If you do not specify an **exceed-action** in the policy-map, it defaults to drop and the violate-action follows.

The PFC QoS does not support the **bandwidth**, **priority**, **queue-limit**, **random-detect**, or **set** keywords in policy-map classes.

## Examples

This example shows how to create a policy map named **max-pol-ipp5** that uses a previously configured class map named **ipp5**, how to configure trust-received IP-precedence values, and how to configure a maximum-capacity aggregate policer and a microflow policer:

```
Router# configure terminal
Enter configuration commands, one per line! End with CNTL/11
Router(config)# policy-map max-pol-ipp5
Router(config-pmap)# class ipp5
Router(config-pmap-c)# trust ip-precedence
Router(config-pmap-c)# police 200000000 2000000 8000000 conform-action set-prec-transmit
6 exceed-action policed-dscp-transmit
Router(config-pmap-c)# police flow 10000000 10000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)# end
Router#
```

## Related Commands

Command	Description
<b>class-map</b>	Accesses the QoS class map configuration mode to configure QoS class maps.
<b>class (policy-map)</b>	Specifies the name of the class that has a policy that you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy.
<b>service-policy</b>	Attaches a policy map to an interface.

Command	Description
<a href="#">show class-map</a>	Displays class-map information.
<a href="#">show policy-map</a>	Displays information about the policy map.
<a href="#">show policy-map interface</a>	Displays the statistics and the configurations of the input and output policies that are attached to an interface.

## port access-map

To create a port access map or enter port access-map command mode, use the **port access-map** command. To remove a mapping sequence or the entire map, use the **no** form of this command.

**port access-map** *name* [*seq#*]

**no port access-map** *name* [*seq#*]

Syntax Description	<i>name</i>	Port access-map tag.
	<i>seq#</i>	(Optional) Map sequence number; valid values are 0 to 65535.

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

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** If you enter the sequence number of an existing map sequence, you enter port access-map mode. If you do not specify a sequence number, a number is automatically assigned. You can enter one match clause and one action clause per map sequence.

If you enter the **no port access-map name** [*seq#*] command without entering a sequence number, the whole map is removed.

Once you enter port access-map mode, the following commands are available:

- **action**—Specifies the packet action clause; see the **action** command section.
- **default**—Sets a command to its defaults.
- **end**—Exits from configuration mode.
- **exit**—Exits from the port access-map configuration mode.
- **match**—Specifies the match clause; see the **match** command section.
- **no**—Negates a command or sets its defaults.

**Examples** This example shows how to enter port access-map mode:

```
Router(config)# port access-map ted
Router(config-port-map)#
```

## ■ port access-map

Related Commands	Command	Description
	<b>action</b>	Sets the packet action clause.
	<b>match</b>	Specifies the match clause by selecting one or more ACLs for a VLAN access-map sequence.

# port-channel load-balance

To set the load-distribution method among the ports in the bundle, use the **port-channel load-balance** command. To return to the default settings, use the **no** form of this command.

**port-channel load-balance** *method*

**no port-channel load-balance**

Syntax Description	
	<i>method</i> Load-distribution method; see the “Usage Guidelines” section for a list of valid values.

Defaults	
	<i>method</i> is <b>src-dst-ip</b> .

Command Modes	
	Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Usage Guidelines	
	Valid <i>method</i> values are as follows:

- **dst-ip**—Loads distribution on the destination IP address
- **dst-mac**—Loads distribution on the destination MAC address
- **dst-port**—Loads distribution on the destination port
- **src-dst-ip**—Loads distribution on the source XOR-destination IP address
- **src-dst-mac**—Loads distribution on the source XOR-destination MAC address
- **src-dst-port**—Loads distribution on the source XOR-destination port
- **src-ip**—Loads distribution on the source IP address
- **src-mac**—Loads distribution on the source MAC address
- **src-port**—Loads distribution on the source port

The **port-channel per-module load-balance** command allows you to enable or disable port-channel load-balancing on a per-module basis.

This example shows how to set the load-distribution method to **dst-ip**:

```
Router(config)# port-channel load-balance dst-ip
Router(config)#
```

This example shows how to set the load-distribution method on a specific module:

```
Router(config)# port-channel load-balance dst-ip module 2
Router(config)#
```

#### Related Commands

Command	Description
<a href="#">interface port-channel</a>	Creates a port-channel virtual interface and enters interface configuration mode.
<a href="#">port-channel per-module load-balance</a>	Enables load-distribution on a per-module basis.
<a href="#">show etherchannel</a>	Displays the EtherChannel information for a channel.

## port-channel load-balance mpls

To set the load-distribution method among the ports in the bundle for MPLS packets, use the **port-channel load-balance mpls** command. To return to the default settings, use the **no** form of this command.

**port-channel load-balance mpls {label | label-ip}**

**no port-channel load-balance mpls**

Syntax Description	label	label-ip
	Specifies using the MPLS label to distribute packets; see the “Usage Guidelines” section for additional information.	Specifies using the MPLS label or the IP address to distribute packets; see the “Usage Guidelines” section for additional information.

Defaults	label-ip

Command Modes	Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Usage Guidelines	If you select <b>label</b> , these guidelines apply:
	<ul style="list-style-type: none"> <li>• With only one MPLS label, the last MPLS label is used.</li> <li>• With two or more MPLS labels, the last two labels (up to the fifth label) are used.</li> </ul>
	If you select <b>label-ip</b> , these guidelines apply:
	<ul style="list-style-type: none"> <li>• With IPv4 and three or fewer labels, the source IP address XOR-destination IP address is used to distribute packets.</li> <li>• With four or more labels, the last two labels (up to the fifth label) are used.</li> <li>• With non-IPv4 packets, the distribution method is the same as the <b>label</b> method.</li> </ul>

## ■ port-channel load-balance mpls

---

**Examples**

This example shows how to set the load-distribution method to **label-ip**:

```
Router(config)# port-channel load-balance mpls label-ip
Router(config)#
```

---

**Related Commands**

Command	Description
<a href="#">interface port-channel</a>	Creates a port-channel virtual interface and enters interface configuration mode.
<a href="#">show etherchannel</a>	Displays the EtherChannel information for a channel.

# port-channel min-links

To specify that a minimum number of bundled ports in an EtherChannel is required before the channel can be active, use the **port-channel min-links** command. To return to the default settings, use the **no** form of this command.

**port-channel min-links** *min-num*

**no port-channel min-links**

<b>Syntax Description</b>	<i>min-num</i>	Minimum number of bundled ports in a channel that is required before the channel can be active; valid values are from 2 to 8.
---------------------------	----------------	---

<b>Defaults</b>	<i>min-num</i> is <b>1</b> .
-----------------	------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	<p>This command is supported on LACP (802.3ad) ports only. More than one LACP secondary port channel can belong to the same channel group. This command is applied to all port channels in the same group.</p> <p>If fewer links than the specified number are available, the port-channel interface does not become active.</p> <p>Use the <b>show running-config</b> command to verify the configuration.</p>
-------------------------	---

<b>Examples</b>	<p>This example shows how to specify that a minimum number of bundled ports in an EtherChannel is required before the channel can be active:</p>
-----------------	--

```
Router(config-if)# port-channel min-links 3
Router(config-if)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show running-config</a>	Displays the status and configuration of the module or Layer 2 VLAN.

## port-channel per-module load-balance

To enable load-distribution on a per-module basis, use the **port-channel per-module load-balance** command. To return to the default settings, use the **no** form of this command.

**port-channel per-module load-balance**

**no port-channel per-module load-balance**

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

**Defaults** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **port-channel load-balance method module slot** command is supported on DFC systems only. The **port-channel per-module load-balance** command allows you to enable or disable port-channel load-balancing on a per-module basis. You can enter the **port-channel load-balance method module slot** command to specify the load-balancing method on a specific module after you have entered the **port-channel per-module load-balance** command.

**Examples** This example shows how to enable load balancing on a per-module basis:

```
Router(config)# port-channel per-module load-balance
Router(config)#
```

Related Commands	Command	Description
	<a href="#">interface port-channel</a>	Creates a port-channel virtual interface and enters interface configuration mode.
	<a href="#">port-channel load-balance module</a>	Enables load-distribution on a specific module.
	<a href="#">show etherchannel</a>	Displays the EtherChannel information for a channel.

# power enable

To turn on power for the modules, use the **power enable** command. To power down a module, use the **no** form of this command.

**power enable** {**module** *slot*}

**no power enable** {**module** *slot*}

<b>Syntax Description</b>	<b>module</b> <i>slot</i>	Specifies a module slot number; see the “Usage Guidelines” section for valid values.
---------------------------	---------------------------	--

<b>Defaults</b>	Enabled
-----------------	---------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	When you enter the <b>no power enable module</b> <i>slot</i> command to power down a module, the module’s configuration is not saved.
	When you enter the <b>no power enable module</b> <i>slot</i> command to power down an empty slot, the configuration is saved.
	The <i>slot</i> argument designates the module number. Valid values for <i>slot</i> depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values for the module number are from 1 to 13.

<b>Examples</b>	This example shows how to turn on the power for a module that was previously powered down:
-----------------	--

```
Router(config)# power enable module 5
Router(config)#
```

This example shows how to power down a module:

```
Router(config)# no power enable module 5
Router(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show power</a>	Displays information about the power status.

# power inline

To configure the administrative mode of the inline power on an interface, use the **power inline** command.

```
power inline {auto [max max-milli-watts]} | never | {static [max max-milli-watts]}
```

Syntax Description	auto	Turns on the device discovery protocol and applies power to the device, if found.
	<b>max</b> <i>max-milli-watts</i>	(Optional) Specifies the maximum amount of power that a device connected to a port can consume; valid values are from 4000 to 15400 milliwatts.
	<b>never</b>	Turns off the device discovery protocol and stops supplying power to the device.
	<b>static</b>	Allocates power from the system power pool to a port.

**Defaults** The defaults are as follows:

- **auto**.
- *max-milli-watts* is 15400 milliwatts.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to set the inline power to the off mode on an interface:

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# switchport
Router(config-if)# power inline never
```

This example shows how to allocate power from the system power pool to a port:

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# switchport
Router(config-if)# power inline static max 15000
```

Related Commands	Command	Description
	<a href="#">show power</a>	Displays information about the power status.

# power redundancy-mode

To set the power-supply redundancy mode, use the **power redundancy-mode** command.

**power redundancy-mode { combined | redundant }**

Syntax Description	combined	Specifies no redundancy (combine power-supply outputs).
	redundant	Specifies redundancy (either power supply can operate the system).

**Defaults** **redundant**

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to set the power supplies to the no-redundancy mode:

```
Router(config)# power redundancy-mode combined
Router(config)#
```

This example shows how to set the power supplies to the redundancy mode:

```
Router(config)# power redundancy-mode redundant
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show power</a>	Displays information about the power status.

## priority-queue cos-map

To map CoS values to the receive and transmit strict-priority queues, use the **priority-queue cos-map** command. To return to the default mapping, use the **no** form of this command.

```
priority-queue cos-map queue-id cos1 [cos2 [cos3 [cos4 [cos5 [cos6 [cos7 [cos8]]]]]]]
```

### Syntax Description

<i>queue-id</i>	Queue number; the valid value is <b>1</b> .
<i>cos1</i>	CoS value; valid values are from 0 to 7.
<i>... cos8</i>	(Optional) CoS values; valid values are from 0 to 7.

### Defaults

The default mapping is queue 1 is mapped to CoS 5 for the following receive and transmit strict-priority queues:

- 1p1q4t receive queues
- 1p1q0t receive queues
- 1p1q8t receive queues
- 1p2q2t transmit queues
- 1p3q8t transmit queues
- 1p7q8t transmit queues
- 1p3q1t transmit queues
- 1p2q1t transmit queues

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

When mapping CoS values to the strict-priority queues, note the following information:

- The queue number is always **1**.
- You can enter up to 8 CoS values to map to the queue.

---

**Examples**

This example shows how to map CoS value 7 to the strict-priority queues on Gigabit Ethernet port 1/1:

```
Router(config-if)# priority-queue cos-map 1 7
Router(config-if)#
```

---

**Related Commands**

Command	Description
<a href="#">show queueing interface</a>	Displays queueing information.

---

# priority-queue queue-limit

To set the priority-queue size on an interface, use the **priority-queue queue-limit** command.

**priority-queue queue-limit** *weight*

Syntax Description	<i>weight</i>	Priority-queue size weight; valid values are from 1 and 100 percent.
--------------------	---------------	--

Defaults	The default settings are as follows:
----------	--------------------------------------

- Global QoS is enabled—15
- Global QoS is disabled—0

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Usage Guidelines	See the <i>Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY</i> for a list of modules that support this command.
------------------	--

Examples	This example shows how to allocate available buffer space to a priority queue:
----------	--

```
Router(config-if)# priority-queue queue-limit 15
Router(config-if)#
```

Related Commands	Command	Description
	<a href="#">show queueing interface</a>	Displays queueing information.

# private-vlan

To configure PVLANS and the association between a PVLAN and a secondary VLAN, use the **private-vlan** command. To return to the default settings, use the **no** form of this command.

**private-vlan** { **isolated** | **community** | **primary** }

**private-vlan association** *secondary-vlan-list* | { **add** *secondary-vlan-list* } |  
{ **remove** *secondary-vlan-list* }

**no private-vlan** { **isolated** | **community** | **primary** }

**no private-vlan association**

Syntax Description		
<b>isolated</b>		Designates the VLAN as an isolated PVLAN.
<b>community</b>		Designates the VLAN as a community PVLAN.
<b>primary</b>		Designates the VLAN as the primary PVLAN.
<b>association</b>		Creates an association between a secondary VLAN and a primary VLAN.
<i>secondary-vlan-list</i>		Number of the secondary VLAN.
<b>add</b>		Associates a secondary VLAN to a primary VLAN.
<b>remove</b>		Clears the association between a secondary VLAN and a primary VLAN.

**Defaults** No PVLANS are configured.

**Command Modes** config-VLAN submode

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** You cannot configure PVLANS on a port-security port.  
If you enter a **pvlan** command on a port-security port, this error message is displayed:  
Command rejected: Gix/y is Port Security enabled port1

Within groups of 12 ports (1–12, 13–24, 25–36, and 37–48), do not configure the ports as isolated or as community VLAN ports when one of the ports is a trunk, a SPAN destination, or a promiscuous private VLAN port. If one port is a trunk, a SPAN destination, or a promiscuous private VLAN port, any isolated or community VLAN configuration for the other ports within the 12 ports is inactive. To reactivate the ports, remove the isolated or community VLAN-port configuration and enter the **shutdown** and **no shutdown** commands.

**Caution**

If you enter the **shutdown** command and then the **no shutdown** command in the config-vlan mode on a PVLAN (primary or secondary), the PVLAN type and association information is deleted. You will have to reconfigure the VLAN to be a PVLAN.

**Note**

This restriction applies to Ethernet 10-Mb, 10/100-Mb, and 100-Mb modules except WS-X6548-RJ-45 and WS-X6548-RJ-21.

You cannot configure VLAN 1 or VLANs 1001 to 1005 as PVLANS.

VTP does not support PVLANS. You must configure PVLANS on each device where you want PVLAN ports.

The *secondary-vlan-list* argument cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single PVLAN ID or a hyphenated range of PVLAN IDs. The *secondary-vlan-list* parameter can contain multiple community VLAN IDs.

The *secondary-vlan-list* argument can contain only one isolated VLAN ID. A PVLAN is a set of private ports that are characterized by using a common set of VLAN number pairs. Each pair is made up of at least two special unidirectional VLANs and is used by isolated ports and/or by a community of ports to communicate with routers.

An isolated VLAN is a VLAN that is used by isolated ports to communicate with promiscuous ports. An isolated VLAN's traffic is blocked on all other private ports in the same VLAN. Its traffic can only be received by standard trunking ports and promiscuous ports that are assigned to the corresponding primary VLAN.

A promiscuous port is defined as a private port that is assigned to a primary VLAN.

A primary VLAN is defined as the VLAN that is used to convey the traffic from the routers to customer end stations on private ports.

A community VLAN is defined as the VLAN that carries the traffic among community ports and from community ports to the promiscuous ports on the corresponding primary VLAN.

You can specify only one isolated *vlan-id*, while multiple community VLANs are allowed. Isolated and community VLANs can only be associated with one VLAN. The associated VLAN list may not contain primary VLANs. Similarly, you cannot configure a VLAN that is already associated to a primary VLAN 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 Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY* for additional configuration guidelines.

**Examples**

This example shows how to create a PVLAN relationship between the primary VLAN 14, the isolated VLAN 19, and the community VLANs 20 and 21:

```
Router(config) # vlan 19
Router(config-vlan) # private-vlan isolated
Router(config) # vlan 20
Router(config-vlan) # private-vlan community
Router(config-vlan) # private-vlan community
Router(config) # vlan 14
Router(config-vlan) # private-vlan primary
Router(config-vlan) # private-vlan association 19-21
```

This example shows how to remove an isolated VLAN and community VLAN 20 from the PVLAN association:

```
Router(config) # vlan 14
Router(config-vlan) # private-vlan association remove 18,20
Router(config-vlan) #
```

This example shows how to remove a PVLAN relationship and delete the primary VLAN. The associated secondary VLANs are not deleted.

```
Router(config-vlan) # no private-vlan 14
Router(config-vlan) #
```

**Related Commands**

Command	Description
<a href="#">show vlan</a>	Displays VLAN information.
<a href="#">show vlan private-vlan</a>	Displays PVLAN information.

## private-vlan mapping

To create a mapping between the primary and the secondary VLANs so that both VLANs share the same primary VLAN SVI, use the **private-vlan mapping** command. To remove all PVLAN mappings from the SVI, use the **no** form of this command.

```
private-vlan mapping [{secondary-vlan-list | {add secondary-vlan-list |
  {remove secondary-vlan-list}}}]
```

```
no private-vlan mapping
```

Syntax Description	
<i>secondary-vlan-list</i>	(Optional) VLAN ID of the secondary VLANs to map to the primary VLAN.
<b>add</b>	(Optional) Maps the secondary VLAN to the primary VLAN.
<b>remove</b>	(Optional) Removes the mapping between the secondary VLAN and the primary VLAN.

**Defaults** No PVLAN SVI mapping is configured.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

The **private-vlan mapping** command affects traffic that is switched in the software on the PISA.

The *secondary-vlan-list* argument cannot contain spaces; it can contain multiple comma-separated items. Each item can be a single PVLAN ID or a hyphenated range of PVLAN IDs.

This command is valid in the interface configuration mode of the primary VLAN.

The SVI of the primary VLAN is created at Layer 3.

Traffic that is received on the secondary VLAN is routed by the SVI of the primary VLAN.

The SVIs of existing secondary VLANs do not function and are considered as down after you enter this command.

A secondary SVI can only be mapped to one primary SVI. If you configure the primary VLAN as a secondary VLAN, all the SVIs that are specified in this command are brought down.

If you configure a mapping between two VLANs that do not have a valid Layer 2 association, the mapping configuration does not take effect.

**Examples**

This example shows how to map the interface of VLAN 20 to the SVI of VLAN 18:

```
Router(config)# interface vlan 18
Router(config-if)# private-vlan mapping 18 20
Router(config-if)#
```

This example shows how to permit routing of secondary VLAN-ingress traffic from PVLANS 303 through 307, 309, and 440 and verify the configuration:

```
Router# configure terminal
Router(config)# interface vlan 202
Router(config-if)# private-vlan mapping add 303-307,309,440
Router(config-if)# end
Router# show interfaces private-vlan mapping
Interface Secondary VLAN Type
-----
vlan505 303 community
vlan505 304 community
vlan505 305 community
vlan505 306 community
vlan505 307 community
vlan505 309 community
vlan505 440 isolated
Router#
```

This example shows the displayed error message 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.

```
Router(config)# interface vlan 19
Router(config-if)# private-vlan mapping 19 add 21
Command rejected: The interface for VLAN 54 is already mapped as s secondary1
Router(config-if)#
```

This example shows how to remove all PVLAN mappings from the SVI of VLAN 19:

```
Router(config)# interface vlan 19
Router(config-if)# no private-vlan mapping
Router(config-if)#
```

**Related Commands**

Command	Description
<a href="#">show interfaces private-vlan mapping</a>	Displays the information about the PVLAN mapping for VLAN SVIs.
<a href="#">show vlan</a>	Displays VLAN information.
<a href="#">show vlan private-vlan</a>	Displays PVLAN 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 keywords or arguments.

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

**Command Modes** MST configuration submode

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** If you do not map VLANs to the same instance as the associated primary VLAN when you exit the MST configuration submode, a warning message displays and lists the secondary VLANs that are not mapped to the same instance as the associated primary VLAN. The **private-vlan synchronize** command automatically maps all secondary VLANs to the same instance as the associated primary VLANs.

**Examples** This example 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:

```
Router(config)# spanning-tree mst configuration
Router(config-mst)# instance 1 vlan 2
Router(config-mst)# exit
These secondary vlans are not mapped to the same instance as their primary:
-> 3
```

This example shows how to initialize PVLAN synchronization:

```
Router(config-mst)# private-vlan synchronize
Router(config-mst)#
```

Related Commands	Command	Description
	<a href="#">show</a>	Verifies the MST configuration.
	<a href="#">show spanning-tree mst</a>	Displays information about the MST protocol.

# process-min-time percent

To specify the minimum percentage of CPU process time OSPF takes before trying to release the CPU for other processes, use the **process-min-time percent** command. To return to the default settings, use the **no** form of this command.

**process-min-time percent** *percent*

**no process-min-time**

## Syntax Description

<i>percent</i>	Percentage of CPU process time to be used before trying to release the CPU for other processes; valid values are from 1 to 100.
----------------	---

## Defaults

*percent* is **25**.

## Command Modes

Router configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines



### Note

Use this command under the direction of Cisco TAC only.

This command is supported by OSPFv2 and OSPFv3.

Use the **process-min-time** command to configure the minimum percentage of the process maximum time. Once the percentage has been exceeded, CPU control may be given to a higher priority process.

The process maximum time is set using the **process-max-time** command. Use the **process-min-time** command with the **process-max-time** command.

## Examples

This example shows how to set the percentage of CPU process time to be used before releasing the CPU:

```
Router> configure terminal
Router(configure)# router ospf
Router(config-router)# process-min-time percent 35
Router(config-router)#
```

This example shows how to return to the default setting:

```
Router> configure terminal
Router(configure)# router rip
Router(config-router)# no process-min-time
Router(config-router)#
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>process-max-time</b>	Configures the amount of time after which a process should voluntarily yield to another process.

---

# rcv-queue bandwidth

To define the bandwidths for ingress (receive) WRR queues through scheduling weights, use the **rcv-queue bandwidth** command. To return to the default settings, use the **no** form of this command.

```
rcv-queue bandwidth weight-1 ... weight-n
```

```
no rcv-queue bandwidth
```

<b>Syntax Description</b>	<i>weight-1 ... weight-n</i> WRR weights; valid values are from 0 to 255.
---------------------------	---

<b>Defaults</b>	The defaults are as follows: <ul style="list-style-type: none"> <li>• QoS enabled—4:255</li> <li>• QoS disabled—255:1</li> </ul>
-----------------	--

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	<p>This command is not supported on Catalyst 6500 series switches that are configured with a Supervisor Engine 2.</p> <p>This command is supported on 2q8t and 8q8t ports only.</p> <p>You can configure up to seven queue weights.</p>
-------------------------	---

<b>Examples</b>	This example shows how to allocate a three-to-one bandwidth ratio:
-----------------	--

```
Router(config-if)# rcv-queue bandwidth 3 1
Router(config-if)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">rcv-queue queue-limit</a>	Sets the size ratio between the strict-priority and standard receive queues.
	<a href="#">show queueing interface</a>	Displays queueing information.

## rcv-queue cos-map

To map the CoS values to the standard receive-queue drop thresholds, use the **rcv-queue cos-map** command. To remove the mapping, use the **no** form of this command.

```
rcv-queue cos-map queue-id threshold-id cos-1 ... cos-n
```

```
no rcv-queue cos-map queue-id threshold-id
```

Syntax Description	
<i>queue-id</i>	Queue ID; the valid value is 1.
<i>threshold-id</i>	Threshold ID; valid values are from 1 to 4.
<i>cos-1</i> ... <i>cos-n</i>	CoS values; valid values are from 0 to 7.

### Defaults

The defaults are listed in [Table 2-30](#).

**Table 2-30 CoS-to-Standard Receive Queue Map Defaults**

queue	threshold	cos-map	queue	threshold	cos-map
With QoS Disabled			With QoS Enabled		
1	1	0,1, 2,3,4,5,6,7	1	1	0,1
1	2		1	2	2,3
1	3		1	3	4
1	4		1	4	6,7
2	1	5	2	1	5

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

The *cos-n* value is defined by the module and port type. When you enter the *cos-n* value, note that the higher values indicate higher priorities.

Use this command on trusted ports only.

For additional information on configuring receive-queue thresholds, see the QoS chapter in the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*.

---

**Examples**

This example shows how to map the CoS values 0 and 1 to threshold 1 in the standard receive queue:

```
Router (config-if)# rcv-queue cos-map 1 1 0 1
  cos-map configured on: Gi4/4 Gi4/5
Router(config-if)#
```

---

**Related Commands**

Command	Description
<a href="#">show queueing interface</a>	Displays queueing information.

---

## rcv-queue queue-limit

To set the size ratio between the strict-priority and standard receive queues, use the **rcv-queue queue-limit** command. To return to the default settings, use the **no** form of this command.

**rcv-queue queue-limit** {*q-limit-1*} {*q-limit-2*}

**no rcv-queue queue-limit**

Syntax Description	
<i>q-limit-1</i>	Standard queue weight; valid values are from 1 and 100 percent.
<i>q-limit-2</i>	Strict-priority queue weight; see the “Usage Guidelines” section for valid values.

Defaults	The defaults are as follows: <ul style="list-style-type: none"> <li>• <b>80</b> percent is for low priority.</li> <li>• <b>20</b> percent is for strict priority.</li> </ul>
----------	--

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Valid strict-priority weight values are from 1 to 100 percent, except on 1p1q8t ingress LAN ports, where valid values for the strict-priority queue are from 3 to 100 percent.

The **rcv-queue queue-limit** command configures ports on a per-ASIC basis.

Estimate the mix of strict-priority-to-standard traffic on your network (for example, 80-percent standard traffic and 20-percent strict-priority traffic) and use the estimated percentages as queue weights.

**Examples** This example shows how to set the receive-queue size ratio for Gigabit Ethernet interface 1/2:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
Router(config)# interface gigabitethernet 1/2
Router(config-if)# rcv-queue queue-limit 75 15
Router(config-if)# end
Router#
```

Related Commands	Command	Description
	<a href="#">show queueing interface</a>	Displays queueing information.

## rcv-queue random-detect

To specify the minimum and maximum threshold for the specified receive queues, use the **rcv-queue random-detect** command. To return to the default settings, use the **no** form of this command.

```
rcv-queue random-detect { max-threshold | min-threshold } queue-id threshold-percent-1 ...
threshold-percent-n
```

```
no rcv-queue random-detect { max-threshold | min-threshold } queue-id
```

### Syntax Description

<b>max-threshold</b>	Specifies the maximum threshold.
<b>min-threshold</b>	Specifies the minimum threshold.
<i>queue-id</i>	Queue ID; the valid value is <b>1</b> .
<i>threshold-percent-1</i> <i>threshold-percent-n</i>	Threshold weights; valid values are from 1 to 100 percent.

### Defaults

The defaults are as follows:

- **min-threshold**—80 percent
- **max-threshold**—20 percent

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

This command is supported on 1p1q8t and 8q8t ports only.

The 1p1q8t interface indicates one strict queue and one standard queue with eight thresholds. The 8q8t interface indicates eight standard queues with eight thresholds. The threshold in the strict-priority queue is not configurable.

Each threshold has a low- and a high-threshold value. The threshold values are a percentage of the receive-queue capacity.

For additional information on configuring receive-queue thresholds, refer to the QoS chapter in the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*.

---

**Examples**

This example shows how to configure the low-priority receive-queue thresholds:

```
Router (config-if)# rcv-queue random-detect max-threshold 1 60 100
Router (config-if)#
```

---

**Related Commands**

Command	Description
<a href="#">show queueing interface</a>	Displays queueing information.

---

## rcv-queue threshold

To configure the drop-threshold percentages for the standard receive queues on 1p1q4t and 1p1q0t interfaces, use the **rcv-queue threshold** command. To return the thresholds to the default settings, use the **no** form of this command.

```
rcv-queue threshold queue-id threshold-percent-1 ... threshold-percent-n
```

```
no rcv-queue threshold
```

### Syntax Description

<i>queue-id</i>	Queue ID; the valid value is <b>1</b> .
<i>threshold- percent-1</i> ... <i>threshold- percent-n</i>	Threshold ID; valid values are from 1 to 100 percent.

### Defaults

The defaults for the 1p1q4t and 1p1q0t configurations are as follows:

- QoS assigns all traffic with CoS 5 to the strict-priority queue.
- QoS assigns all other traffic to the standard queue.

The default for the 1q4t configuration is that QoS assigns all traffic to the standard queue.

If you enable QoS, the following default thresholds apply:

- 1p1q4t interfaces have this default drop-threshold configuration:
  - Frames with CoS 0, 1, 2, 3, 4, 6, or 7 go to the standard receive queue.
  - Using standard receive-queue drop threshold 1, the Catalyst 6500 series switch drops incoming frames with CoS 0 or 1 when the receive-queue buffer is 50 percent or more full.
  - Using standard receive-queue drop threshold 2, the Catalyst 6500 series switch drops incoming frames with CoS 2 or 3 when the receive-queue buffer is 60 percent or more full.
  - Using standard receive-queue drop threshold 3, the Catalyst 6500 series switch drops incoming frames with CoS 4 when the receive-queue buffer is 80 percent or more full.
  - Using standard receive-queue drop threshold 4, the Catalyst 6500 series switch drops incoming frames with CoS 6 or 7 when the receive-queue buffer is 100 percent full.
  - Frames with CoS 5 go to the strict-priority receive queue (queue 2), where the Catalyst 6500 series switch drops incoming frames only when the strict-priority receive-queue buffer is 100 percent full.
- 1p1q0t interfaces have this default drop-threshold configuration:
  - Frames with CoS 0, 1, 2, 3, 4, 6, or 7 go to the standard receive queue. The Catalyst 6500 series switch drops incoming frames when the receive-queue buffer is 100 percent full.
  - Frames with CoS 5 go to the strict-priority receive queue (queue 2), where the Catalyst 6500 series switch drops incoming frames only when the strict-priority receive-queue buffer is 100 percent full.



#### Note

The 100-percent threshold may be actually changed by the module to 98 percent to allow BPDU traffic to proceed. The BPDU threshold is factory set at 100 percent.

## rcv-queue threshold

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

The *queue-id* value is always **1**.

A value of **10** indicates a threshold when the buffer is 10 percent full.

Always set threshold 4 to 100 percent.

Receive thresholds take effect only on ports whose trust state is **trust cos**.

Configure the 1q4t receive-queue tail-drop threshold percentages with the **wrr-queue threshold** command.

**Examples** This example shows how to configure the receive-queue drop thresholds for Gigabit Ethernet interface 1/1:

```
Router(config-if)# rcv-queue threshold 1 60 75 85 100
Router(config-if)#
```

Related Commands	Command	Description
	<b>show queueing interface</b>	Displays queueing information.
	<b>wrr-queue threshold</b>	Configures the drop-threshold percentages for the standard receive and transmit queues on 1q4t and 2q2t interfaces.

# reassign

To define the number of consecutive number of SYNs for a new connection that will go unanswered before the connection is attempted to a different real server, use the **reassign** command. To change the maximum number of connections to the default settings, use the **no** form of this command.

**reassign** *threshold*

**no reassign**

<b>Syntax Description</b>	<i>threshold</i>	Number of unanswered TCP SYNs that will be directed to a real server before the connection is reassigned to a different real server; valid values are from 1 to 4.
---------------------------	------------------	--

<b>Defaults</b>	<i>threshold</i> is 3.
-----------------	------------------------

<b>Command Modes</b>	Real server configuration submode
----------------------	-----------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	If you do not specify the <i>threshold</i> value, the default value of the reassignment threshold is used.
-------------------------	--

**Examples** This example shows how to define the reassignment threshold:

```
Router(config-if)# reassign 4
Router(config-if)#
```

This example shows how to revert to the default value:

```
Router(config-if)# no reassign
Router(config-if)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>faildetect numconns</b>	Specifies the conditions that indicate a server failure.
	<b>inservice (real server)</b>	Enables the real server for use by the Cisco IOS SLB feature.
	<b>retry</b>	Defines the amount of time that must elapse before a connection is attempted to a failed server.
	<b>maxconns (real server configuration submode)</b>	Limits the number of active connections to the real server.

# redundancy

To enter redundancy configuration mode, use the **redundancy** command. From this mode, you can enter the main CPU submode to manually synchronize the configurations that are used by the two supervisor engines.

## redundancy

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

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

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Once you enter redundancy configuration mode, these options are available:

- **exit**—Exits from redundancy configuration mode.
- **main-cpu**—Enters the main CPU submode.
- **no**—Negates a command or sets its defaults.

From the main CPU submode, you can use the **auto-sync** command to use all of the redundancy commands that are applicable to the main CPU.

To select the type of redundancy mode, use the **mode** command.

NSF with SSO redundancy mode supports IPv4. NSF with SSO redundancy mode does not support IPv6, IPX, and MPLS.

---

**Examples**

This example shows how to enter redundancy mode:

```
Router (config)# redundancy  
Router(config-r)#
```

This example shows how to enter the main CPU submode:

```
Router (config)# redundancy  
Router (config-r)# main-cpu  
Router (config-r-mc)#
```

---

**Related Commands**

Command	Description
<a href="#">auto-sync</a>	Enables automatic synchronization of the configuration files in NVRAM.
<a href="#">mode</a>	Sets the redundancy mode.

# 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** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Before using this command, see the “Performing a Fast Software Upgrade (FSU)” section of the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY* 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 new Cisco IOS image. The modules are reset and the module software is downloaded from the new active supervisor engine.

The old active supervisor engine reboots with the new image and becomes the redundant supervisor engine.

**Examples** This example shows how to switch over manually from the active to the standby supervisor engine:

```
Router# redundancy force-switchover
Router#
```

Related Commands	Command	Description
	<a href="#">mode</a>	Sets the redundancy mode.
	<a href="#">redundancy</a>	Enters redundancy configuration mode.
	<a href="#">show redundancy</a>	Displays RF information.

# reload

To reload the entire Catalyst 6500 series switch, use the **reload** command.

**reload** [*text* | **in** [*hh:mm*] [*text*] | **at** *hh:mm* [*month day* | *day month*] [*text*] | **cancel**]

Syntax Description	
<i>text</i>	(Optional) Reason for the reload; the string can be from 1 to 255 characters.
<b>in</b> [ <i>hh:mm</i> ]	(Optional) Delays a Catalyst 6500 series switch reload for a specific amount of time.
<b>at</b> <i>hh:mm</i>	(Optional) Schedules a Catalyst 6500 series switch reload to take place at the specified time (using a 24-hour clock).
<i>month</i>	(Optional) Name of the month; any number of characters in a unique string.
<i>day</i>	(Optional) Number of the day; valid values are from 1 to 31.
<b>cancel</b>	(Optional) Cancels a scheduled reload.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **reload** command stops the system. If the system is set to restart on error, it reboots itself. Use the **reload** command after you enter configuration information into a file and the file is saved to the startup configuration.

When you schedule a reload to occur at a later time (using the **in** keyword), it must take place within approximately 24 days.

When specifying the reload time (using the **at** keyword), if you specify the month and day, the reload takes place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within approximately 24 days.

If you modify your configuration file, the Catalyst 6500 series switch prompts you to save the configuration. During a save operation, the Catalyst 6500 series switch asks you if you want to proceed with the save if the CONFIG\_FILE environment variable points to a startup configuration file that no longer exists. If you say “yes” in this situation, the Catalyst 6500 series switch goes to setup mode upon reload.

You can use the **at** keyword if the system clock has been set on the MSM (either through NTP, the hardware calendar, or manually). To schedule reloads across several MSMs to occur simultaneously, you must synchronize the time on each MSM with NTP.

To display information about a scheduled reload, use the **show reload** command.

**Examples**

This example shows how to reload the Catalyst 6500 series switch immediately:

```
Router# reload
Router#
```

This example shows how to reload the Catalyst 6500 series switch in 10 minutes:

```
Router# reload in 10
Router# Reload scheduled for 44:57:08 PDT Fri Apr 54 4996 (in 40 minutes)
Proceed with reload? [confirm]
Router#
```

This example shows how to reload the Catalyst 6500 series switch at 1:00 p.m. today:

```
Router# reload at 13:00
Router# Reload scheduled for 43:00:00 PDT Fri Apr 54 4996 (in 4 hour and 5 minutes)
Proceed with reload? [confirm]
Router#
```

This example shows how to reload the Catalyst 6500 series switch on April 20 at 2:00 a.m.:

```
Router# reload at 02:00 apr 20
Router# Reload scheduled for 05:00:00 PDT Sat Apr 50 4996 (in 38 hours and 9 minutes)
Proceed with reload? [confirm]
Router#
```

This example shows how to cancel a pending reload:

```
Router# reload cancel
%Reload cancelled1
Router#
```

**Related Commands**

Command	Description
<b>copy</b> <b>system:running-config</b> <b>nvrnram:startup-config</b>	Saves configuration changes to the startup configuration.
<b>show reload</b>	Displays the reload status on the router.

# remote command

To execute a Catalyst 6500 series switch command directly on the switch console or a specified module without having to log into the Catalyst 6500 series switch first, use the **remote command** command.

**remote command** {{ **module num** } | **standby-rp** | **switch** } *command*

Syntax Description	Parameter	Description
	<b>module num</b>	Specifies the module to access; see the “Usage Guidelines” section for valid values.
	<b>standby-rp</b>	Specifies the standby route processor.
	<b>switch</b>	Specifies the active switch processor.
	<i>command</i>	Command to be executed.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **module num** keyword and argument designate the module number. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values are from 1 to 13. The **module num** keyword and argument are supported on the standby supervisor engine only.

When you execute the **remote command switch** command, the prompt changes to Switch-sp#.

This command is supported on the supervisor engine only.

This command does not support command completion, but you can use shortened forms of the command (for example, entering **sh** for **show**).

**Examples** This example shows how to execute the **show calendar** command from the standby route processor:

```
Router# remote command standby-rp show calendar
Switch-sp#
09:55:50 UTC Mon Nov 45 5004
Router#
```

Related Commands	Command	Description
	<a href="#">remote login</a>	Accesses the Catalyst 6500 series switch console or a specific module.

# remote login

To access the Catalyst 6500 series switch console or a specific module, use the **remote login** command.

**remote login** { **module num** } | **standby-rp** | **switch** }

Syntax Description	module num	standby-rp	switch
	Specifies the module to access; see the “Usage Guidelines” section for valid values.	Specifies the standby route processor.	Specifies the active switch processor.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines



When you enter the **attach** or **remote login** command to access another console from your switch, if you enter global or interface configuration mode commands, the switch might reset.

The **module num** keyword and argument designate the module number. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values are from 1 to 13. The **module num** keyword and argument are supported on the standby supervisor engine only.

When you execute the **remote login module num** command, the prompt changes depending on the type of module to which you are connecting.

When you execute the **remote login standby-rp** command, the prompt changes to Router-sdby#.

When you execute the **remote login switch** command, the prompt changes to Switch-sp#.

The **remote login module num** command is identical to the **attach** command.

There are two ways to end the session:

- You can enter the **exit** command as follows:

```
Switch-sp# exit
```

```
[Connection to Switch closed by foreign host]
```

```
Router#
```

- You can press **Ctrl-C** three times as follows:

```
Switch-sp# ^C
Switch-sp# ^C
Switch-sp# ^C
Terminate remote login session? [confirm] y
[Connection to Switch closed by local host]
Router#
```

## Examples

This example shows how to perform a remote login to a specific module:

```
Router# remote login module 1
Trying Switch 111
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
```

```
Switch-sp#
```

This example shows how to perform a remote login to the Catalyst 6500 series switch processor:

```
Router# remote login switch
Trying Switch 111
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
Switch-sp#
```

This example shows how to perform a remote login to the standby route processor:

```
Router# remote login standby-rp
Trying Switch 111
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
Router-sdby#
```

## Related Commands

Command	Description
<a href="#">attach</a>	Connects to a specific module from a remote location.

# remote-span

To configure a VLAN as an RSPAN VLAN, use the **remote-span** command. To remove the RSPAN designation, use the **no** form of this command.

## remote-span

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

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

**Command Modes** config-VLAN mode

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command is not supported in the VLAN database mode.

You can enter the **show vlan remote-span** command to display the RSPAN VLANs in the Catalyst 6500 series switch.

**Examples** This example shows how to configure a VLAN as an RSPAN VLAN:

```
Router(config-vlan)# remote-span
Router(config-vlan)
```

This example shows how to remove the RSPAN designation:

```
Router(config-vlan)# no remote-span
Router(config-vlan)
```

Related Commands	Connect	Description
	<b>show vlan remote-span</b>	Displays a list of RSPAN VLANs.

# reset

To leave the proposed new VLAN database, remain in VLAN configuration mode, and reset the proposed new database so that it is identical to the current VLAN database, use the **reset** command.

**reset**

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

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

**Command Modes** VLAN configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to cause the proposed new VLAN database to be abandoned and reset to the current VLAN database:

```
Router(vlan)# reset
RESET completed
Router(vlan)#
```

# retry

To define the amount of time that must elapse before a connection is attempted to a failed server, use the **retry** command. To change the connection-reassignment threshold and client threshold to the default settings, use the **no** form of this command.

**retry** *retry-value*

**no retry**

<b>Syntax Description</b>	<i>retry-value</i>	Amount of time, in seconds, that must elapse after the detection of a server failure before a new connection is attempted to the server; valid values are from 1 to 3600.
---------------------------	--------------------	---

<b>Defaults</b>	<i>retry-value</i> is <b>60</b> .
-----------------	-----------------------------------

<b>Command Modes</b>	Real server configuration submode
----------------------	-----------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to define the retry timer:

```
Router(config-if)# retry 145
Router(config-if)#
```

This example shows how to revert to the default value:

```
Router(config-if)# no retry
Router(config-if)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>faildetect numconns</b>	Specifies the conditions that indicate a server failure.
	<b>inservice (real server)</b>	Enables the real server for use by the Cisco IOS SLB feature.
	<b>maxconns (real server configuration submode)</b>	Limits the number of active connections to the real server.

# revision

To set the revision number for the MST configuration, 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>	Revision number for the configuration; valid values are from 0 to 65535.
--------------------	----------------	--

Defaults	<i>version</i> is <b>0</b> .
----------	------------------------------

Command Modes	MST configuration submode
---------------	---------------------------

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Usage Guidelines	Two Catalyst 6500 series switches that have the same configuration but different revision numbers are considered to be part of two different regions.
------------------	---



Caution

Be careful when using the **revision** command to set the revision number of the MST configuration because a mistake can put the switch in a different region.

Examples	This example shows how to set the revision number of the MST configuration:
----------	---

```
Router(config-mst)# revision 5
Router(config-mst)#
```

Related Commands	Command	Description
	<b>instance</b>	Maps a VLAN or a set of VLANs to an MST instance.
	<b>name (MST configuration submode)</b>	Sets the name of an MST region.
	<b>show</b>	Verifies the MST configuration.
	<b>show spanning-tree</b>	Displays information about the spanning-tree state.
	<b>spanning-tree mst configuration</b>	Enters MST-configuration submode.

## rmon alarm

To set an alarm on any MIB object, use the **rmon alarm** command. To disable the alarm, use the **no** form of this command.

**rmon alarm** *number variable interval* { **delta** | **absolute** } **rising-threshold** *value* [*event-number*]  
**falling-threshold** *value* [*event-number*] [**owner** *string*]

**no rmon alarm** *number*

<b>Syntax Description</b>	<i>number</i>	Alarm number that is identical to the alarmIndex in the alarmTable in the RMON MIB; valid values are from 1 to 65535.
	<i>variable</i>	MIB object to monitor; this value translates into the alarmVariable that is used in the alarmTable of the RMON MIB.
	<i>interval</i>	Time in seconds that the alarm monitors the MIB variable. This value is identical to the alarmInterval that is used in the alarmTable of the RMON MIB; valid values are from 1 to 4294967295.
	<b>delta</b>	Specifies the change between MIB variables; this value affects the alarmSampleType in the alarmTable of the RMON MIB.
	<b>absolute</b>	Specifies each MIB variable directly; this value affects the alarmSampleType in the alarmTable of the RMON MIB.
	<b>rising-threshold</b> <i>value</i>	Specifies the value at which the alarm is triggered; valid values are from -2147483648 to 2147483647.
	<i>event-number</i>	(Optional) Event number to trigger when the rising or falling threshold exceeds its limit. This value is identical to the alarmRisingEventIndex or the alarmFallingEventIndex in the alarmTable of the RMON MIB; valid values are from 1 to 65535.
	<b>falling-threshold</b> <i>value</i>	Specifies the value at which the alarm is reset; valid values are from -2147483648 to 2147483647.
	<b>owner</b> <i>string</i>	(Optional) Specifies the owner for the alarm; this value is identical to the alarmOwner in the alarmTable of the RMON MIB.

**Defaults** No alarms are configured.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

You must specify the MIB object as a dotted decimal value after the entry sequence (for example, *ifEntry.10.1*). You cannot specify the variable name and the instance (for example, *ifInOctets.1*) or the entire dotted decimal notation. The argument must be of the form *entry.integer.instance*.

To disable the RMON alarms, you must use the **no** form of the command on each configured alarm. For example, enter the **no rmon alarm 1** command, where the 1 identifies which alarm is to be removed.

Refer to RFC 1757 for more information about the RMON alarm group.

In the configuration that is shown in the example, the alarm monitors the MIB variable *ifEntry.20.1* once every 20 seconds until the alarm is disabled and checks the change in the variable's rise or fall. If the *ifEntry.20.1* value shows a MIB counter increase of 15 or more, such as from 100000 to 100015, the alarm is triggered. The alarm triggers event number 1, which is configured with the **rmon event** command. Possible events include a log entry or an SNMP trap. If the *ifEntry.20.1* value changes by 0 (falling-threshold 0), the alarm is reset and can be triggered again.

### Examples

This example shows how to configure an RMON alarm:

```
Router(config)# rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1
falling-threshold 0
owner jjohnson
```

Related Commands	Command	Description
	<b>rmon</b>	Enables RMON on an Ethernet interface.
	<b>rmon event</b>	Adds or removes an event in the RMON-event table that is associated with an RMON-event number.
	<b>show rmon</b>	Displays the current RMON agent status on the router.

## rmon event

To add or remove an event in the RMON-event table that is associated with an RMON-event number, use the **rmon event** command. To disable RMON on the interface, use the **no** form of this command.

**rmon event** *number* [**log**] [**trap** *community*] [**description** *string*] [**owner** *string*]

**no rmon event** *number*

Syntax Description		
	<i>number</i>	Assigned event number that is identical to the eventIndex in the eventTable in the RMON MIB; valid values are from 1 to 65535.
	<b>log</b>	(Optional) Generates an RMON log entry when the event is triggered and sets the eventType in the RMON MIB to log or log-and-trap.
	<b>trap</b> <i>community</i>	(Optional) Specifies the SNMP community string that is used for this trap.
	<b>description</b> <i>string</i>	(Optional) Specifies a description of the event that is identical to the event description in the eventTable of the RMON MIB.
	<b>owner</b> <i>string</i>	(Optional) Specifies the owner of this event that is identical to the eventOwner in the eventTable of the RMON MIB.

**Defaults** No alarms are configured.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Refer to RFC 1757 for more information about the RMON MIB.

Use the **trap** *community* keyword and argument to configure the setting of the eventType in the RMON MIB for this row as either snmp-trap or log-and-trap. This value is identical to the eventCommunityValue in the eventTable in the RMON MIB.

---

**Examples**

This example shows how to add an event to the RMON-event table:

```
Router(config)# rmon event 1 log trap eventtrap description "High ifOutErrors" owner
sdurham
```

This example configuration creates RMON-event number 1, which is defined as High ifOutErrors, and generates a log entry when the event is triggered by an alarm. The user sdurham owns the row that is created in the event table by this command. This configuration also generates an SNMP trap when the event is triggered.

---

**Related Commands**

Command	Description
<b>rmon</b>	Enables RMON on an Ethernet interface.
<b>rmon alarm</b>	Sets an alarm on any MIB object.
<b>show rmon</b>	Displays the current RMON agent status on the router.

## route-converge-interval

To configure the time interval after which the old FIB entries are purged, use the **route-converge-interval** command. To return to the default settings, use the **no** form of this command.

**route-converge-interval** *seconds*

<b>Syntax Description</b>	<i>seconds</i>	Time interval after which the old FIB entries are purged; valid values are from 60 to 3600 seconds.
---------------------------	----------------	---

<b>Defaults</b>	<i>seconds</i> is <b>120</b> seconds (2 minutes).
-----------------	---

<b>Command Modes</b>	Main CPU submode
----------------------	------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	The time interval for route-converge delay is needed to simulate the route-converge time when routing protocols restart on switchover.
-------------------------	--

<b>Examples</b>	This example shows how to set the time interval for the route-converge delay:
-----------------	---

```
Router(config)# redundancy
Router(config-red)# main-cpu
Router(config-red-main)# route-converge-interval 90
Router(config-red-main)#
```

This example shows how to return to the default time interval for the route-converge delay:

```
Router(config)# redundancy
Router(config-red)# main-cpu
Router(config-red-main)# no route-converge-interval
Router(config-red-main)#
```

---

**Related Commands**

Command	Description
<a href="#">redundancy</a>	Enters redundancy configuration mode.

---

# router

To enable a routing process, use the **router** command. To terminate a routing process, use the **no** form of this command.

```
router {bgp as-num} | {eigrp as-num} | {isis process-id} | {ospf process-id [vrf vrf-id]}
```

```
no router ospf process-id
```

Syntax Description		
<b>bgp</b> <i>as-num</i>	Specifies an autonomous BGP-system number; valid values are from 1 to 65535.	
<b>eigrp</b> <i>as-num</i>	Specifies an autonomous EIGRP-system number; valid values are from 1 to 65535.	
<b>isis</b> <i>routing-area-tag</i>	Specifies an ISO routing area designation.	
<b>ospf</b> <i>process-id</i>	Specifies an internally used identification parameter for the routing process; valid values are from 1 to 65535.	
<b>vrf</b> <i>vrf-id</i>	(Optional) Specifies a VRF instance name.	

**Defaults** No OSPF routing process is enabled or defined.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** When you specify a *process-id*, it is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process.

You can specify multiple OSPF routing processes in each router.

**Examples** This example shows how to configure an OSPF routing process and assign a process number of 109:

```
Router(config)# router ospf 109
Router(config)#
```

This example shows how to configure an OSPF routing process and assign a process number of 109 for a specific VRF instance:

```
Router(config)# router ospf 109 vrf 109
Router(config)#
```

Related Commands	Command	Description
	<b>nsf</b>	Enables and configures Cisco NSF.

# scheduler allocate

To guarantee the CPU time for the process tasks, use the **scheduler allocate** command. To return to the default settings, use the **no** form of this command.

**scheduler allocate** *interrupt-time process-time*

**no scheduler allocate**

Syntax Description	
<i>interrupt-time</i>	Integer (in microseconds) that limits the maximum number of microseconds to spend on fast switching within any one network-interrupt context; valid values are from 400 to 60000 microseconds.
<i>process-time</i>	Integer (in microseconds) that guarantees the minimum number of microseconds to spend at the process level when network interrupts are disabled; valid values are from 100 to 4000.

## Defaults

The defaults are as follows:

- *interrupt-time* is **4000** microseconds.
- *process-time* is **800** microseconds.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines



### Caution

We recommend that you do not change the default settings.

Entering the **scheduler allocate** command without arguments is the same as entering the **no scheduler allocate** or the **default scheduler allocate** command.

## Examples

This example shows how to make 20 percent of the CPU time available for the process tasks:

```
Router-config# scheduler allocate 2000 500
Router-config#
```

## service counters max age

To set the time interval for retrieving statistics, use the **service counters max age** command. To return to the default settings, use the **no** form of this command.

**service counters max age** *seconds*

**no service counters max age**

<b>Syntax Description</b>	<i>seconds</i>	Maximum age of the statistics retrieved from the CLI or SNMP; valid values are from 0 to 60 seconds.
---------------------------	----------------	--

<b>Defaults</b>	<i>seconds</i> is 5 seconds.
-----------------	------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines



#### Note

If you decrease the time interval for retrieving statistics from the default setting (5 seconds), traffic congestion may result in situations where frequent SNMP (SMNP bulk) retrievals occur.

If you configure the *seconds* value between 6 and 9 seconds, the counter update occurs at the 10-second default to ensure that the system is not too busy computing statistics. If the statistics collection uses more than 20 percent of the CPU time, the system automatically increases the time that the statistics process sleeps between counter updates.

If you configure the *seconds* value between 0 and 5 seconds, and if the CPU utility is low, the counter updates occur after the configured delay seconds which ensures that the system load is at 20 percent.

For example, if the statistics calculation time takes 4 seconds, and you have configured the service maximum age to 5 seconds, the period between statistics collections will be 20 seconds (the collection period equals the duration multiplied by 5) regardless of what you configured, which ensures that the statistics collection does not increase the CPU utility.

### Examples

This example shows how to set the time interval for retrieving statistics:

```
Router(config)# service counters max age 10
Router(config)#
```

This example shows how to return to the default setting:

```
Router(config)# no service counters max age
Router(config)#
```

# service-policy

To attach a policy map to an interface, use the **service-policy** command. To remove a policy map from an interface, use the **no** form of this command.

**service-policy** { **input** | **output** } *policy-map-name*

**no service-policy** { **input** | **output** } *policy-map-name*

Syntax Description	Command	Description
	<b>input</b> <i>policy-map-name</i>	Specifies a previously configured input-policy map.
	<b>output</b> <i>policy-map-name</i>	Specifies a previously configured output-policy map.

**Defaults** No policy map is attached.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Do not attach a service policy to a port that is a member of an EtherChannel.

Although the CLI allows you to configure PFC-based QoS on the WAN ports on the OC-12 ATM OSMs and on the WAN ports on the channelized OSMs, PFC-based QoS is not supported on the WAN ports on these OSMs. OSMs are not supported on Catalyst 6500 series switches that are configured with a Supervisor Engine 32 PISA.

PFC QoS supports the optional **output** keyword only on VLAN interfaces. You can attach both an input-policy map and an output-policy map to a VLAN interface.

**Examples** This example shows how to attach a policy map to a Fast Ethernet interface:

```
Router(config)# interface fastethernet 5/20
Router(config-if)# service-policy input pmap1
Router(config-if)#
```

Related Commands	Command	Description
	<a href="#">class-map</a>	Accesses the QoS class map configuration mode to configure QoS class maps.
	<a href="#">policy-map</a>	Accesses QoS policy-map configuration mode to configure the QoS policy map.

## service-policy (control-plane)

To attach a policy map to a control plane for aggregate control plane services, use the **service-policy** command. To remove a service policy from a control plane, 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	Applies the specified service policy to the packets that are entering the control plane.
	output	Applies the specified service policy to the packets that are exiting the control plane and enables the Catalyst 6500 series switch to silently discard packets.
	<i>policy-map-name</i>	Name of a service policy map (created using the <b>policy-map</b> command) to be attached.

**Defaults** No service policy is specified.

**Command Modes** Control-plane configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The *policy-map-name* can be a maximum of 40 alphanumeric characters.

After entering the **control-plane** command, you should use the **service-policy** command to configure a QoS policy. This policy is attached to the control plane interface for aggregate control plane services, which can control the number or rate of packets that are going to the process level.

Silent mode allows a router that is running Cisco IOS software to operate without sending any system messages. If a packet that is destined for the router is discarded for any reason, users will not receive an error message. Some events that will not generate error messages are as follows:

- Traffic that is being transmitted to a port in which that router is not listening
- A connection to a legitimate address and port that is rejected because of a malformed request

**Examples** This example shows 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:

```
Router(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
! Allow 40141415 trusted host traffic1
Router(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
! Rate limit all other Telnet traffic1
Router(config)# access-list 140 permit tcp any any eq telnet
```

```

! Define class-map "telnet-class1"
Router(config)# class-map telnet-class
Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map control-plane-policy
Router(config-pmap)# class telnet-class
Router(config-pmap-c)# police 80000 conform transmit exceed drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
! Define aggregate control plane service for the active Route Processor1
Router(config)# control-plane
Router(config-cp)# service-policy input control-plane-policy
Router(config-cp)# exit

```

This example shows how to configure trusted networks with source addresses 3.3.3.0 and 4.4.4.0 to receive Internet Control Message Protocol (ICMP) port-unreachable responses without constraint, while allowing all remaining ICMP port-unreachables to be dropped:

```

Router(config)# access-list 141 deny icmp host 3.3.3.0 0.0.0.255 any port-unreachable
! Allow 4141410 trusted network traffic1
Router(config)# access-list 141 deny icmp host 4.4.4.0 0.0.0.255 any port-unreachable
! Rate limit all other ICMP traffic1
Router(config)# access-list 141 permit icmp any any port-unreachable
Router(config)# class-map icmp-class
Router(config-cmap)# match access-group 141
Router(config-cmap)# exit
Router(config)# policy-map control-plane-out-policy
! Drop all traffic that matches the class "icmp-class1"
Router(config-pmap)# class icmp-class
Router(config-pmap-c)# drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# control-plane
! Define aggregate control plane service for the active route processor1
Router(config-cp)# service-policy output control-plane-policy
Router(config-cp)# exit

```

#### Related Commands

Command	Description
<a href="#">control-plane</a>	Enters 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.
<a href="#">policy-map</a>	Accesses QoS policy-map configuration mode to configure the QoS policy map.
<a href="#">show policy-map control-plane</a>	Displays the configuration either of a class or of all classes for the policy map of a control plane.

## session slot

To open a session with a module (for example, the NAM), use the **session slot** command.

```
session slot mod {processor processor-id}
```

Syntax Description	<i>mod</i>	Slot number.
	<b>processor</b> <i>processor-id</i>	Specifies the processor ID.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** To end the session, enter the **quit** command.  
This command allows you to use the module-specific CLI.

**Examples** This example shows how to open a session with an MSM (module 4):

```
Router# session slot 4 processor 2
Router#
```

## set cos cos-inner (policy-map configuration)

To set the 802.1Q prioritization bits in the trunk VLAN tag of a QinQ-translated outgoing packet with the priority value from the inner customer-edge VLAN tag, use the **set cos cos-inner** command. To return to the default settings, use the **no** form of this command.

**set cos cos-inner**

**no set cos cos-inner**

### Syntax Description

This command has no keywords or arguments.

### Defaults

P bits are copied from the outer provider-edge VLAN tag.

### Command Modes

Policy-map class configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

This command is supported on the Gigabit Ethernet WAN interfaces on Catalyst 6500 series switches that are configured with an OSM-2+4GE-WAN+ OSM module only.

OSMs are not supported on Catalyst 6500 series switches that are configured with a Supervisor Engine 32.

The 802.1P prioritization bits are used in the VLAN tag for QoS processing.

When the router copies the double-tagged QinQ packets to the destination interface, by default it uses the P bits from the outer (provider) VLAN tag. To preserve the P bits that are in the inner (customer) VLAN tag, use the **set cos cos-inner** command.

For the **set cos cos-inner** command to be effective, you must configure the appropriate interface or subinterface as a trusted interface using the **mls qos trust** command. Otherwise, the interface or subinterface defaults to being untrusted, where the Layer 2 interface zeroes out the P bits of the incoming packets before the **set cos cos-inner** command can copy them to the outer VLAN tag.

The **set cos cos-inner** command is supported only for the subinterfaces that are configured with an inner (customer) VLAN. The **set cos cos-inner** command is not supported for the subinterfaces that use the **out-range** keyword on the **bridge-domain (subinterface configuration)** command or that are not configured with any form of the **bridge-domain (subinterface configuration)** command.

This behavior remains when you configure the **set cos cos-inner** command on a policy that is applied to a main interface. The **set cos cos-inner** command affects the subinterfaces that are configured with a specific inner VLAN but it does not affect the subinterfaces that are not configured with any VLAN or that are configured with the **out-range** keyword.

**Examples**

This example shows how to configure a policy map for voice traffic that uses the P bits from the inner VLAN tag:

```
Router(config-pmap-c)# set cos cos-inner
Router(config-pmap-c)#
```

This example shows how to configure the default policy map class to reset to its default value:

```
Router(config-pmap-c)# no set cos cos-inner
Router(config-pmap-c)#
```

This example shows the system message that appears when you attempt to apply a policy to a subinterface that is configured with the **bridge-domain (subinterface configuration)** command:

```
Router(config-if)# bridge-vlan 32 dot1q-tunnel out-range
Router(config-if)# service-policy output cos1
```

```
%bridge-vlan 35 does not have any inner-vlan configured! 'set cos cos-inner' is not supported
```

```
Router(config-if)#
```

**Related Commands**

Command	Description
<b>bridge-domain (subinterface configuration)</b>	Binds a PVC to the specified <i>vlan-id</i> .
<b>class-map</b>	Accesses the QoS class map configuration mode to configure QoS class maps.
<b>mode dot1q-in-dot1q access-gateway</b>	Enables a Gigabit Ethernet WAN interface to act as a gateway for QinQ VLAN translation.
<b>policy-map</b>	Accesses QoS policy-map configuration mode to configure the QoS policy map.
<b>service-policy</b>	Attaches a policy map to an interface.
<b>set ip dscp (policy-map configuration)</b>	Marks a packet by setting the IP DSCP in the ToS byte.
<b>set ip precedence (policy-map configuration)</b>	Sets the precedence value in the IP header.
<b>show policy-map</b>	Displays information about the policy map.
<b>show policy-map interface</b>	Displays the statistics and the configurations of the input and output policies that are attached to an interface.

## set ip dscp (policy-map configuration)

To mark a packet by setting the IP DSCP in the ToS byte, use the **set ip dscp** command. To remove a previously set IP DSCP, use the **no** form of this command.

**set ip dscp** *ip-dscp-value*

**no set ip dscp** *ip-dscp-value*

<b>Syntax Description</b>	<i>ip-dscp-value</i>	IP DSCP value; valid values are from 0 to 63. See the “Usage Guidelines” section for additional information.
---------------------------	----------------------	--

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

<b>Command Modes</b>	QoS policy-map configuration
----------------------	------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	<p>You can enter reserved keywords <b>EF</b> (expedited forwarding), <b>AF11</b> (assured forwarding class AF11), and <b>AF12</b> (assured forwarding class AF12) instead of numeric values for <i>ip-dscp-value</i>.</p> <p>After the IP DSCP bit is set, other QoS services can operate on the bit settings.</p> <p>You cannot mark a packet by the IP precedence using the <b>set ip precedence (policy-map configuration)</b> command and then mark the same packet with an IP DSCP value using the <b>set ip dscp</b> command.</p> <p>The network gives priority (or some type of expedited handling) to marked traffic. Typically, you set IP precedence at the edge of the network (or administrative domain); data is queued based on the precedence. WFQ can speed up handling for high-precedence traffic at congestion points. WRED ensures that high-precedence traffic has lower loss rates than other traffic during traffic congestion.</p> <p>The <b>set ip precedence (policy-map configuration)</b> command is applied when you create a service policy in QoS policy-map configuration mode. This service policy is not attached to an interface or to an ATM virtual circuit. See the <b>service-policy</b> command for information on attaching a service policy to an interface.</p>
-------------------------	--

When configuring policy-map class actions, note the following:

- For hardware-switched traffic, PFC QoS does not support the **bandwidth**, **priority**, **queue-limit**, or **random-detect** policy-map class commands. You can configure these commands because they can be used for software-switched traffic.
- PFC QoS does not support the **set mpls** or **set qos-group** policy-map class commands.
- PFC QoS supports the **set ip dscp** and **set ip precedence** policy-map class commands (see the “Configuring Policy Map Class Marking” section in the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*).

- You cannot do all three of the following in a policy-map class:
  - Mark traffic with the **set ip dscp** or **set ip precedence (policy-map configuration)** commands
  - Configure the trust state
  - Configure policing

In a policy-map class, you can either mark traffic with the **set ip dscp** or **set ip precedence (policy-map configuration)** commands or do one or both of the following:

- Configure the trust state
- Configure policing

## Examples

This example shows how to set the IP DSCP ToS byte to 8 in the policy map called policy1:

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set ip dscp 8
```

All packets that satisfy the match criteria of class1 are marked with the IP DSCP value of 8. How packets that are marked with the IP DSCP value of 8 are treated is determined by the network configuration.

This example shows that after you configure the settings that are shown for voice packets at the edge of the network, all intermediate routers are then configured to provide low-latency treatment to the voice packets:

```
Router(config)# class-map voice
Router(config-cmap)# match ip dscp ef
Router(config)# policy qos-policy
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 24
```

## Related Commands

Command	Description
<b>policy-map</b>	Accesses QoS policy-map configuration mode to configure the QoS policy map.
<b>service-policy</b>	Attaches a policy map to an interface.
<b>show policy-map</b>	Displays information about the policy map.
<b>show policy-map interface</b>	Displays the statistics and the configurations of the input and output policies that are attached to an interface.

## set ip precedence (policy-map configuration)

To set the precedence value in the IP header, use the **set ip precedence** command. To leave the precedence value at the current setting, use the **no** form of this command.

**set ip precedence** *ip-precedence-value*

**no set ip precedence**

<b>Syntax Description</b>	<i>ip-precedence-value</i>	Precedence-bit value in the IP header; valid values are from 0 to 7. See <a href="#">Table 2-31</a> for a list of value definitions.
---------------------------	----------------------------	--

<b>Defaults</b>	This command is disabled by default.
-----------------	--------------------------------------

<b>Command Modes</b>	QoS policy-map configuration
----------------------	------------------------------

<b>Command History</b>	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	<a href="#">Table 2-31</a> lists the value definitions for precedence values in the IP header. They are listed from least to most important.
-------------------------	--

**Table 2-31 Value Definitions for IP Precedence**

Values	Definitions
0	routine
1	priority
2	immediate
3	flash
4	flash-override
5	critical
6	internet
7	network

After the IP-precedence bits are set, other QoS services, such as WFQ and WRED, operate on the bit settings.

The network priorities (or some type of expedited handling) mark traffic through the application of WFQ or WRED at points downstream in the network. Typically, you set IP precedence at the edge of the network (or administrative domain); data is queued based on the precedence. WFQ can speed up handling for certain precedence traffic at congestion points. WRED can ensure that certain precedence traffic has lower loss rates than other traffic during traffic congestion.

The **set ip precedence** command is applied when you create a service policy in QoS policy-map configuration mode. This service policy is not attached to an interface or to an ATM virtual circuit. See the [service-policy](#) command for information on attaching a service policy to an interface.

### Examples

This example shows how to set the IP precedence to 5 for packets that satisfy the match criteria of the class map called class1:

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set ip precedence 5
```

All packets that satisfy the match criteria of class1 are marked with the IP precedence value of 5. How packets that are marked with the IP-precedence value of 5 are treated is determined by the network configuration.

### Related Commands

Command	Description
<a href="#">policy-map</a>	Accesses QoS policy-map configuration mode to configure the QoS policy map.
<a href="#">service-policy</a>	Attaches a policy map to an interface.
<a href="#">show policy-map</a>	Displays information about the policy map.
<a href="#">show policy-map interface</a>	Displays the statistics and the configurations of the input and output policies that are attached to an interface.

# set mpls experimental

To set the experimental value, use the **set mpls experimental** command. To return to the default settings, use the **no** form of this command.

```
set mpls experimental {{ imposition | topmost } experimental-value }
```

Syntax Description		
	<b>imposition</b>	Specifies the experimental-bit value on IP to MPLS or MPLS input in all newly imposed labels.
	<b>topmost</b>	Specifies the experimental-bit value on the topmost label on the input or output flows.
	<i>experimental-value</i>	Experimental-bit value; valid values are from 0 to 7.

**Defaults** This command is disabled by default.

**Command Modes** QoS policy-map configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to set the experimental-bit value on the topmost label on input or output:

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set mpls experimental topmost 5
```

## set qos-group

To set the trusted state of a Layer 2 WAN interface, use the **set qos-group** command. To return to the default settings, use the **no** form of this command.

```
set qos-group group-value {cos | prec}
```

Syntax Description	<i>group-value</i>	QoS group value; valid values are from 0 to 99.
	<b>cos</b>	Specifies that the CoS bits in incoming frames are trusted and derives the internal DSCP value from the CoS bits.
	<b>prec</b>	Specifies that the ToS bits in the incoming packets contain an IP-precedence value and derives the internal DSCP value from the IP-precedence bits.

**Defaults** This command is disabled by default.

**Command Modes** QoS policy-map configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command is entered in Pipe mode on the MPLS input to select the egress queue. This command is supported on WAN interfaces only. Use the **mls qos trust** command to set the trusted state on LAN interfaces.

**Examples** This example shows how to set the trusted state of an interface to IP precedence:

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set qos-group 54 prec
Router(config-if)#
```

# show

To verify the MST configuration, use the **show** command.

**show [current | pending]**

Syntax Description	current	(Optional) Displays the current configuration that is used to run MST.
	pending	(Optional) Displays the edited configuration that will replace the current configuration.

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

**Command Modes** MST configuration submode

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The display output from the **show pending** command is the edited configuration that will replace the current configuration if you enter the **exit** command to exit MST configuration mode. Entering the **show** command with no arguments displays the pending configurations.

**Examples** This example shows how to display the edited configuration:

```
Router(config-mst)# show pending
Pending MST configuration
Name      [zorglub]
Version   34445
Instance  Vlans Mapped
-----
0         4004-4096
5         4040, 4050, 4030, 4040, 4050, 4060, 4070, 4080, 4090, 4400, 4440
         4450
3         4-4009, 4044-4049, 4054-4059, 4034-4039, 4044-4049, 4054-4059
         4064-4069, 4074-4079, 4084-4089, 4094-4099, 4404-4409, 4444-4449
         4454-4000
-----
Router(config-mst)#
```

This example shows how to display the current configuration:

```
Router(config-mst)# show current
Current MST configuration
Name []
Revision 0
Instance Vlans mapped
-----
0 4-4094
-----
```

#### Related Commands

Command	Description
<a href="#">instance</a>	Maps a VLAN or a set of VLANs to an MST instance.
<a href="#">name (MST configuration submode)</a>	Sets the name of an MST region.
<a href="#">revision</a>	Sets the revision number for the MST configuration.
<a href="#">show spanning-tree mst</a>	Displays the information about the MST protocol.
<a href="#">spanning-tree mst configuration</a>	Enters MST-configuration submode.

# show adjacency

To display information about the hardware Layer 3-switching adjacency table, use the **show adjacency** command.

```
show adjacency [{interface interface-number} | {null interface-number} | {port-channel number}
| {vlan vlan-id} | detail | internal | summary]
```

Syntax Description	
<i>interface</i>	(Optional) Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , <b>ge-wan</b> , and <b>atm</b> .
<i>interface-number</i>	(Optional) Module and port number; see the “Usage Guidelines” section for valid values.
<b>null</b> <i>interface-number</i>	(Optional) Specifies the null interface; the valid value is <b>0</b> .
<b>port-channel</b> <i>number</i>	(Optional) Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 256.
<b>vlan</b> <i>vlan-id</i>	(Optional) Specifies the VLAN; valid values are from 1 to 4094.
<b>detail</b>	(Optional) Displays the information about the protocol detail and timer.
<b>internal</b>	(Optional) Displays the information about the internal data structure.
<b>summary</b>	(Optional) Displays a summary of CEF-adjacency information.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

Hardware Layer 3-switching adjacency statistics are updated every 60 seconds.

The information that is contained in the **show adjacency** commands includes the following:

- Protocol interface.
- Type of routing protocol that is configured on the interface.
- Interface address.
- Method of adjacency that was learned.
- 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:

```
Router# show adjacency
Protocol Interface          Address
IP       FastEthernet5/3      47515015514 (3045)
IP       FastEthernet5/3      475150155155 (44)
Router#
```

This example shows how to display a summary of adjacency information:

```
Router# show adjacency summary
Adjacency Table has 5 adjacencies
  Interface          Adjacency Count
  FastEthernet5/3    5
Router#
```

This example shows how to display protocol detail and timer information:

```
Router# show adjacency detail
Protocol Interface          Address
IP       FastEthernet5/3      47515015514 (3045)
                                                0 packets, 0 bytes
                                                000000000FF950000380000000000000
                                                00000000000000000000000000000000
                                                00605C865B5800D0BB0F980B0800
ARP      03:58:45
IP       FastEthernet5/3      475150155155 (44)
                                                0 packets, 0 bytes
                                                000000000FF950000380000000000000
                                                00000000000000000000000000000000
                                                00804C93804000D0BB0F980B0800
ARP      03:58:06
Router#
```

This example shows how to display adjacency information for a specific interface:

```
Router# show adjacency fastethernet 2/3
Protocol Interface Address
IP FastEthernet5/3 47515015514 (3045)
IP FastEthernet5/3 475150155155 (44)
Router#
```

---

**Related Commands**

Command	Description
<a href="#">show mls cef adjacency</a>	Displays information about the MLS-hardware Layer 3-switching adjacency node.

---

# show arp

To display the ARP table, use the **show arp** command.

**show arp**

---

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

---

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

---

**Command Modes** EXEC

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Examples** This example shows how to display the ARP table:

```
Router> show arp
Protocol  Address           Age (min)  Hardware Addr  Type   Interface
Internet  475150155144      4          0090154561d800 ARPA   Vlan5
Internet  47515015514       58         006015c8615b58 ARPA   Vlan5
Internet  475150155155     459        008014c9318040 ARPA   Vlan5
Router>
```

# show asic-version

To display the ASIC version for a specific module, use the **show asic-version** command.

**show asic-version slot number**

Syntax Description	<i>number</i>	Module number.
--------------------	---------------	----------------

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** In the **show asic-version** command output, the ASIC types are as follows:

- Lyra—Layer 2 forwarding engine
- Hyperion—Packet rewrite, multicast, and SPAN engine
- Polaris—Layer 3 CEF engine
- Pinnacle—4-port Gigabit Ethernet interface
- R2D2—Network interface (with combinations of 10/100/1000Mbps and 10Gbps), a receive packet buffer interface, a transmit packet buffer interface as well as an interface to a further upstream ASIC or FPGA.
- Titan—Packet rewrite and replication engine
- Vela—Constellation bus interface

**Examples** This example shows how to display the ASIC type and version for a specific module:

```
Router# show asic-version slot 1
Module in slot 4 has 3 type(s) of ASICs
  ASIC Name      Count    Version
  PINNACLE       4        (510)
  MEDUSA         4        (510)
  TITAN          4        (014)
Router#
```

## 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.
	<b>chips</b>	(Optional) Displays information about the flash chip.
	<b>fileSYS</b>	(Optional) Displays information about the file system.

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

**Command Modes** User EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display information about the file system status:

```
Router> show bootflash: fileSYS

----- F I L E   S \ S T E M   S T A T U S -----
Device Number = 0
DEVICE INFO BLOCK: bootflash
  Magic Number      = 6887635   File System Vers = 40000   (410)
  Length            = 4000000   Sector Size      = 40000
  Programming Algorithm = 39     Erased State     = FFFFFFFF
  File System Offset = 40000     Length = F40000
  MONLIB Offset     = 400       Length = C658
  Bad Sector Map Offset = 3FFF8   Length = 8
  Squeeze Log Offset = F80000   Length = 40000
  Squeeze Buffer Offset = FC0000  Length = 40000
  Num Spare Sectors = 0
  Spares:
STATUS INFO:
  Writable
  NO File Open for Write
  Complete Stats
  No Unrecovered Errors
  No Squeeze in progress
USAGE INFO:
  Bytes Used      = 947CE8   Bytes Available = 658348
  Bad Sectors    = 0       Spared Sectors  = 0
  OK Files       = 5       Bytes = 947BE8
  Deleted Files  = 0       Bytes = 0
  Files w/Errors = 0       Bytes = 0
Router>
```

This example shows how to display image information:

```
Router> show bootflash:
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
4  11 image    8C5A393A  537E3C   44  5063804 Aug 53 4999 46:48:45 c6msfc-boot-mz
5  11 image    D86EE0AD  957CE8    9  7470636 Sep 50 4999 43:48:49 rp1halley
Router>
```

This example shows how to display all bootflash information:

```
Router> show bootflash: all
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
4  11 image    8C5A393A  537E3C   44  5063804 Aug 53 4999 46:48:45 c6msfc-boot-
mz
5  11 image    D86EE0AD  957CE8    9  7470636 Sep 50 4999 43:48:49 rp1halley

6456088 bytes available (9534696 bytes used)

----- F I L E   S \ S T E M   S T A T U S -----
Device Number = 0
DEVICE INFO BLOCK: bootflash
Magic Number      = 6887635   File System Vers = 40000   (410)
Length            = 4000000   Sector Size      = 40000
Programming Algorithm = 39   Erased State     = FFFFFFFF
File System Offset = 40000    Length = F40000
MONLIB Offset     = 400      Length = C658
Bad Sector Map Offset = 3FFF8   Length = 8
Squeeze Log Offset = F80000   Length = 40000
Squeeze Buffer Offset = FC0000  Length = 40000
Num Spare Sectors = 0
Spares:
STATUS INFO:
Writable
NO File Open for Write
Complete Stats
No Unrecovered Errors
No Squeeze in progress
USAGE INFO:
Bytes Used      = 947CE8   Bytes Available = 658348
Bad Sectors    = 0       Spared Sectors = 0
OK Files       = 5       Bytes = 947BE8
Deleted Files  = 0       Bytes = 0
Files w/Errors = 0       Bytes = 0
Router>
```

# show bootvar

To display information about the BOOT environment variable, use the **show bootvar** command.

## show bootvar

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

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

**Command Modes** User EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **show bootvar** command output depends on how you configure the boot statement as follows:

- If you enter the **boot system flash bootflash:sup720\_image** command in the boot configuration, then the **show bootvar** command output displays the bootflash information.
- If you enter the **boot system flash sup-bootflash:sup720\_image** command in the boot configuration, then the **show bootvar** command output displays the sup-bootflash information. This action is the correct way of configuring the boot statement.

The **show bootvar** command is available from the switch processor CLI and the route processor CLI. From the switch processor CLI, the display is always bootflash. With either the bootflash or the sup-bootflash boot statement, the switch boots correctly. You should use sup-bootflash in the boot configuration statement because the image is stored in the switch processor bootflash; the route processor sees the image as sup-bootflash.

The number displayed after the image name (an example is c6sup12-js-mz.121-13.E,12) indicates the number of times that the Catalyst 6500 series switch tries to reboot the file before giving up.

**Examples** This example shows how to display information about the BOOT environment variable:

```
Router# show bootvar
BOOT variable = sup-bootflash:c6sup45-js-mz1454-431E,45
CONFIG_FILE variable =
BOOTLDR variable = bootflash:c6msfc5-boot-mz1454-431E1bin
Configuration register is 0x5405

Standby is up
Standby has 445640K/48435K bytes of memory1
```

```
Standby BOOT variable = bootflash:c6sup45-js-mz1454-431E,45
Standby CONFIG_FILE variable =
Standby BOOTLDR variable = bootflash:c6msfc5-boot-mz1454-431E1bin
Standby Configuration register is 0x5405
Router#
```

---

**Related Commands**

Command	Description
<a href="#">auto-sync</a>	Enables automatic synchronization of the configuration files in NVRAM.

---

■ show bootvar

# 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}}
```

Syntax Description	
<b>interface</b> <i>interface</i>	Specifies the interface type; valid values are <b>fastethernet</b> and <b>gigabitethernet</b> .
<i>interface-number</i>	Module and port number.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **show cable-diagnostics tdr** command is supported on specific modules. See the *Release Notes for Cisco IOS Release 12.2 ZY Supervisor Engine 32 PISA* for the list of the modules that support TDR.

In the event of an open or shorted cable, the accuracy of length of where the cable is open or shorted is plus or minus 2 meters.

The pair length can be displayed in meters (m), centimeters (cm), or kilometers (km).

If the TDR test has not been run on the port, the following message is displayed:

```
TDR test was never run on Gi5/45
```

**Examples** This example shows how to display the information about the TDR test:

```
Router> show cable-diagnostics tdr interface gigabitethernet8/1
TDR test last run on: February 55 44:48:34
Interface Speed Pair Cable length      Distance to fault  Channel Pair status
-----
Gi8/4      4000  4-5  4    +/- 6 m          N/A                Pair B  Terminated
           3-4  4    +/- 6 m          N/A                Pair A  Terminated
           5-6  4    +/- 6 m          N/A                Pair C  Terminated
           7-8  4    +/- 6 m          N/A                Pair D  Terminated
Router>
```

Table 2-32 describes the fields in the **show cable-diagnostics tdr** command output.

**Table 2-32** show cable-diagnostics tdr Command Output Fields

Field	Description
Interface	Interface tested.
Speed	Current line speed.
Pair	Local pair name.
Cable Length	Cable length and accuracy. The accuracy unit is displayed in meters (m), centimeters (cm), or kilometers (km).
Channel	Pair designation.
Pair status	<p>Pair status displayed is one of the following:</p> <ul style="list-style-type: none"> <li>• Terminated—The link is up.</li> <li>• Shorted—A short is detected on the cable.</li> <li>• Open—An opening is detected on the cable.</li> <li>• Not Completed—The test on the port failed.</li> <li>• Not Supported—The test on the port is not supported.</li> <li>• Broken—The pair is bad—either open or shorted.</li> <li>• ImpedanceMis—The impedance is mismatched.</li> <li>• InProgress—The diagnostic test is in progress.</li> </ul>

#### Related Commands

Command	Description
<b>clear cable-diagnostics tdr</b>	Clears a specific interface or clears all interfaces that support TDR.
<b>test cable-diagnostics</b>	Tests the condition of 10-Gigabit Ethernet links or copper cables on 48-port 10/100/1000 BASE-T modules.

# show catalyst6000

To display the information about the Catalyst 6500 series switch, use the **show catalyst6000** command.

**show catalyst6000 {all | chassis-mac-address | switching-clock | traffic-meter}**

Syntax Description	all	Displays the MAC-address ranges and the current and peak traffic-meter reading.
	<b>chassis-mac-address</b>	Displays the MAC-address range.
	<b>switching-clock</b>	Displays the failure recovery mode of the switching clock.
	<b>traffic-meter</b>	Displays the percentage of the backplane (shared bus) utilization.

Defaults **all**

Command Modes EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** If you enter the **switching-clock** keywords, the Catalyst 6500 series switch displays whether switching of the redundant clock sources on the backplane is allowed if the active clock source fails.

The Catalyst 6500 series switch has either 64 or 1024 MAC addresses that are available to support the software features. You can enter the **show catalyst6000 chassis-mac-address** command to display the MAC-address range on your chassis.

**Examples** This example shows how to display the MAC-address ranges and the current and peak traffic-meter readings:

```
Router> show catalyst6000 all
  chassis MAC addresses: 64 addresses from 000416444160c0 to 000416444160ff
  traffic meter =    0% Never cleared
                 peak =    0% reached at 08:44:38 UTC Wed Mar 49 5003
  switching-clock: clock switchover and system reset is allowed
Router>
```

This example shows how to display the MAC-address ranges:

```
Router# show catalyst6000 chassis-mac-address
  chassis MAC addresses: 4054 addresses from 00d01004c14800 to 00d01004c14c00
Router#
```

This example shows how to display the current and peak traffic-meter readings:

```
Router> show catalyst6000 traffic-meter
  traffic meter = 0%   peak = 0%   at 09:57:58 UTC Mon Nov 6 5000
Router#
```

This example shows how to display the failure recovery mode of the switching clock:

```
Router> show catalyst6000 switching-clock
  switching-clock: clock switchover and system reset is allowed
Router>
```

# 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	
<i>type</i>	(Optional) Interface type that is connected to the neighbors about which you want information; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>port-channel</b> , and <b>vlan</b> .
<i>number</i>	(Optional) Interface number that is connected to the neighbors about which you want information.
<b>detail</b>	(Optional) Displays detailed information about a neighbor (or neighbors) including the network address, the enabled protocols, the hold time, and the software version.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **port-channel** values are from 0 to 282; values from 257 to 282 are supported on the CSM and the FWSM only.

**Examples** This example shows how to display the information about the CDP neighbors:

```
Router# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce   Holdtme    Capability  Platform  Port ID
lab-7506         Eth 0           457        R           7506VXR   Fas 0/0/0
lab-as5300-4     Eth 0           463        R           AS5300    Fas 0
lab-as5300-5     Eth 0           459        R           AS5300    Eth 0
lab-as5300-3     Eth 0           455        R           AS5300    Eth 0
lab-as5300-4     Eth 0           435        R           AS5300    Fas 0/0
lab-3654         Eth 0           440        R S        3634-telcoFas 0/0
008054 5758E0    Eth 0           435        T           CAT3000   4/5
```

Table 2-33 describes the fields that are shown in the example.

**Table 2-33** show cdp neighbors Field Descriptions

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.

This example shows how to display detailed information about your CDP neighbors:

```
Router# show cdp neighbors detail
-----
Device ID: lab-7506
Entry address(es):
  IP address: 4751491469183
Platform: cisco 7506VXR, Capabilities: Router
Interface: Ethernet0, Port ID (outgoing port): FastEthernet0/0/0
Holdtime : 453 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 5800 Software (C5800-P4-M), Version 4514(5)
Copyright (c) 4986-5005 by Cisco Systems, Inc

advertisement version: 5
Duplex: half

-----
Device ID: lab-as5300-4
Entry address(es):
  IP address: 4751491469187
1
1
1
```

Table 2-34 describes the fields that are shown in the example.

**Table 2-34** *show cdp neighbors detail* Field Descriptions

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.

#### Related Commands

Command	Description
<b>show cdp</b>	Displays global CDP information.
<b>show cdp entry</b>	Displays information about a specific neighboring device discovered using CDP.
<b>show cdp interface</b>	Displays information about the interfaces on which CDP is enabled.
<b>show cdp traffic</b>	Displays information about traffic between devices gathered using CDP.

# show cef interface policy-statistics

To display the per-interface traffic statistics, use the **show cef interface policy-statistics** command.

**show cef interface policy-statistics**

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

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

**Command Modes** User EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the per-interface traffic statistics:

```
Router# show cef interface policy-statistics
POS7/0 is up (if_number 7)
Bucket PacketsBytes
4 0 0
5 0 0
3 0 0
4 0 0
5 400 40000
6 0 0
7 0 0
8 0 0
Router#
```

# show class-map

To display class-map information, use the **show class-map** command.

**show class-map** [*class-name*]

<b>Syntax Description</b>	<i>class-name</i> (Optional) Name of the class map.
---------------------------	---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display class-map information for all class maps:

```
Router# show class-map
Class Map match-any class-default (id 0)
  Match any
Class Map match-any class-simple (id 5)
  Match any
Class Map match-all ipp5 (id 4)
  Match ip precedence 5

Class Map match-all agg-5 (id 3)
```

```
Router#
```

This example shows how to display class-map information for a specific class map:

```
Router# show class-map ipp5
Class Map match-all ipp5 (id 4)
  Match ip precedence 5
```

```
Router#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">class-map</a>	Accesses the QoS class map configuration mode to configure QoS class maps.
	<a href="#">show policy-map</a>	Displays information about the policy map.
	<a href="#">show policy-map interface</a>	Displays the statistics and the configurations of the input and output policies that are attached to an interface.

# show counters interface

To display the information about the interface counter, use the **show counters interface** command.

```
show counters interface {type mod/port} [delta]
```

Syntax Description	type	Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>port-channel</b> , <b>pos</b> , <b>atm</b> , <b>null</b> , <b>tunnel</b> , and <b>ge-wan</b> .
	mod/port	Module and port number.
	delta	(Optional) Displays the interface counters values since the last <b>clear counters</b> command.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **show counters interface** command is not supported on SVIs.  
The **show counters interface delta** command displays a detailed list of the last-saved counter values.

**Examples** This example shows how to display the information about the interface counter:

```
Router# show counters interface fastethernet 5/2
64 bit counters:
 01          rxHCTotalPkts = 4
 41          txHCTotalPkts = 4
 51          rxHCUnicastPkts = 0
 31          txHCUnicastPkts = 0
 41          rxHCMulticastPkts = 0
 51          txHCMulticastPkts = 0
 61          rxHCBroadcastPkts = 4
 71          txHCBroadcastPkts = 4
 81          rxHCOctets = 78
 91          txHCOctets = 78
401         rxTxHCPkts64Octets = 0
441         rxTxHCPkts65to457Octets = 5
451         rxTxHCPkts458to555Octets = 0
431         rxTxHCPkts556to544Octets = 0
441         rxTxHCPkts545to4053Octets = 0
451         rxTxHCPkts4054to4548Octets = 0
461         txHCTrunkFrames = 0
471         rxHCTrunkFrames = 0
481         rxHCDropEvents = 0
```

```

35 bit counters:
 01          rxCRCAAlignErrors = 0
 41          rxUndersizedPkts = 0
 51          rxOversizedPkts = 0
 31          rxFragmentPkts = 0
 41          rxJabbers = 0
 51          txCollisions = 0
 61          ifInErrors = 0
 71          ifOutErrors = 0
 81          ifInDiscards = 0
 91          ifInUnknownProtos = 0
401          ifOutDiscards = 0
441          txDelayExceededDiscards = 0
451          txCRC = 0
431          linkChange = 4
441          wrongEncapFrames = 0
All Port Counters
 41          InPackets = 4
 51          InOctets = 78
 31          InUcastPkts = 0
 41          InMcastPkts = 0
 51          InBcastPkts = 4
 61          OutPackets = 4
 71          OutOctets = 78
 81          OutUcastPkts = 0
 91          OutMcastPkts = 0
401          OutBcastPkts = 4
441          AlignErr = 0
451          FCSErr = 0
431          XmitErr = 0
441          RcvErr = 0
451          UnderSize = 0
461          SingleCol = 0
471          MultiCol = 0
481          LateCol = 0
491          ExcessiveCol = 0
501          CarrierSense = 0
541          Runts = 0
551          Giants = 0
531          InDiscards = 0
541          OutDiscards = 0
551          InErrors = 0
561          OutErrors = 0
571          TrunkFramesTx = 0
581          TrunkFramesRx = 0
591          WrongEncap = 0
301          Broadcast_suppression_discards = 0
341          Multicast_suppression_discards = 0
351          Unicast_suppression_discards = 0
331          rxTxHCPkts64Octets = 0
341          rxTxHCPkts65to457Octets = 5
351          rxTxHCPkts458to555Octets = 0
361          rxTxHCPkts556to544Octets = 0
371          rxTxHCPkts545to4053Octets = 0
381          rxTxHCPkts4054to4548Octets = 0
391          DropEvents = 0
401          CRCAlignErrors = 0
441          UndersizedPkts = 0
451          OversizedPkts = 0
431          FragmentPkts = 0
441          Jabbers = 0
451          Collisions = 0
461          DelayExceededDiscards = 0

```

## ■ show counters interface

```

471          bpduOutlost = 0
481          qos0Outlost = 0
491          qos4Outlost = 0
501          qos5Outlost = 0
541          qos3Outlost = 0
551          bpduCbicOutlost = 0
531          qos0CbicOutlost = 0
541          qos4CbicOutlost = 0
551          qos5CbicOutlost = 0
561          qos3CbicOutlost = 0
571          bpduInlost = 0
581          qos0Inlost = 0
591          qos4Inlost = 0
601          qos5Inlost = 0
641          qos3Inlost = 0
651          qos4Inlost = 0
631          qos5Inlost = 0
641          qos6Inlost = 0
651          qos7Inlost = 0
661          pqueInlost = 0
671          Overruns = 0
681          maxIndex = 0

```

Router#

This example shows how to display the values for the interface counters since the last **clear counters** command:

```

Router# show counters interface gigabitethernet5/2 delta
Time since last clear
-----
4d08h
64 bit counters:
01 rxHCTotalPkts = 508473
41 txHCTotalPkts = 5366
51 rxHCUnicastPkts = 444644
31 txHCUnicastPkts = 493
41 rxHCMulticastPkts = 84868
51 txHCMulticastPkts = 5455
61 rxHCBroadcastPkts = 44994
71 txHCBroadcastPkts = 48
81 rxHCOctets = 36964995
1
1
1
Router#

```

## Related Commands

Command	Description
<a href="#">clear counters</a>	Clears the interface counters.

# show diagnostic

To view the test results of the online diagnostics and list the supported test suites, use the **show diagnostic** command.

**show diagnostic bootstrap level**

**show diagnostic content** [*module num*]

**show diagnostic events** [*module num*] [*event-type event-type*]

**show diagnostic** {*ondemand settings*}

**show diagnostic** {*result* [*module num*] [*detail*]}

**show diagnostic schedule** [*module num*]

Syntax Description		
<b>bootstrap level</b>		Displays the coverage level for the configured boot-up diagnostics.
<b>content</b>		Displays test information including test ID, test attributes, and supported coverage test levels for each test and for all modules.
<b>module num</b>		(Optional) Specifies the module number.
<b>events</b>		Displays the event log for the diagnostic events.
<b>event-type event-type</b>		(Optional) Specifies the event type; valid values are <b>error</b> , <b>info</b> , and <b>warning</b> .
<b>ondemand settings</b>		Displays the settings for the ondemand diagnostics.
<b>result</b>		Displays the test results.
<b>detail</b>		(Optional) Displays the test statistics of each test.
<b>schedule</b>		Displays the current scheduled diagnostic tasks.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** If you do not enter a module *num*, information for all modules is displayed. In the command output, the possible testing results are as follows:

- Passed (.)
- Failed (F)
- Unknown (U)

**Examples**

This example shows how to display the test suite and the monitoring interval and test attributes:

```
Router# show diagnostic content module 1
Diagnostic Tests List for Module 4:
Module 4:

Diagnostics test suite attributes:
  M/C/* - Minimal level test / Complete level test / Not applicable
  B/* - Bypass bootup test / Not applicable
  P/* - Per port test / Not applicable
  D/N - Disruptive test / Non-disruptive test
  S/* - Only applicable to standby unit / Not applicable
  X/* - Not a health monitoring test / Not applicable
  F/* - Fixed monitoring interval test / Not applicable
  E/* - Always enabled monitoring test / Not applicable
  A/I - Monitoring is active / Monitoring is inactive

Testing Interval
ID Test Name Attributes (day hh:mm:sslms)
=== =====
 4) TestDummy4 -----> M**D****A 000 00:04:001000
 5) TestDummy5 -----> M**D**FEA 000 00:05:301000
 3) TestGBICIntegrity -----> *BPD****I not configured
 4) TestActiveToStandbyLoopback -----> M**PDS***I not configured
 5) TestLoopback -----> M**PD****I not configured
 6) TestNewLearn -----> M**N****I not configured
 7) TestIndexLearn -----> M**N****I not configured
 8) TestConditionalLearn -----> M**N****I not configured
 9) TestBadBpdu -----> M**D****I not configured
40) TestCapture -----> M**D****I not configured
44) TestProtocolMatch -----> M**D****I not configured
45) TestChannel -----> M**D****I not configured
43) TestDontShortcut -----> M**Nrefer*I not configured
44) TestL3Capture5 -----> M**N****I not configured
45) TestL3VlanMet -----> M**N****I not configured
46) TestIngressSpan -----> M**N****I not configured
47) TestEgressSpan -----> M**N****I not configured
48) TestAclPermit -----> M**N****I not configured
49) TestAclDeny -----> M**D****I not configured
50) TestNetflowInlineRewrite -----> C**PD****I not configured

Router#
```

This example shows how to display the configured boot-up diagnostic level:

```
Router# show diagnostic bootup level
Current Bootup Diagnostic Level = Complete
Router#
```

This example shows how to display the event log for the diagnostics:

```
Router# show diagnostic events

Diagnostic events (storage for 500 events, 40 events recorded)
Event Type (ET):I - Info, W - Warning, E - Error

Time Stamp      ET [Card] Event Message
-----
08/56 45:54:041335 I [4] TestIndexLearn Passed
08/56 45:54:041335 I [4] Diagnostics Passed
08/56 45:54:451544 I [8] TestLoopback Passed
08/56 45:54:451544 I [8] Diagnostics Passed
08/56 46:45:051547 I [4] TestDontLearn Passed
08/56 46:45:051547 I [4] Diagnostics Passed
08/56 46:45:451683 I [8] TestNetflowInlineRewrite Passed
08/56 46:45:451683 I [8] Diagnostics Passed
```

```
08/56 46:45:451507 I [5] TestActiveToStandbyLoopback Passed
08/56 46:45:451507 I [5] Diagnostics Passed
Router#
```

This example shows how to display the settings for the ondemand diagnostics:

```
Router# show diagnostic ondemand settings
Ondemand Run Iteration = 5
Ondemand Action-on-Error = CONTINUE
Router#
```

This example shows how to display the current scheduled diagnostic tasks for the specified slot:

```
Router# show diagnostic schedule module 1
Current Time = 07:55:30 UTC Fri August 5 5005
```

Diagnostic for Module 4:

```
Schedule #4:
  To be run on January 3 5003 53:35
  Test ID(s) to be executed:41
```

```
Schedule #5:
  To be run daily 44:45
  Test ID(s) to be executed:51
```

```
Schedule #3:
  To be run weekly Monday 3:33
  Test ID(s) to be executed:all1
```

Router#

This example shows how to display the testing results for the specified slot:

```
Router# show diagnostic result module 3
```

Current bootup diagnostic level:complete

Module 3:

```
Overall Diagnostic Result for Module 8 :PASS
Diagnostic level at card bootup:complete
```

Test results:(1 = Pass, F = Fail, U = Untested)

4) TestLoopback :

```
Port  4  5  3  4  5  6  7  8  9 40 44 45 43 44 45 46 47 48 49 50 54 55 53 54
-----
      1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1
Port 55 56 57 58 59 30 34 35 33 34 35 36 37 38 39 40 44 45 43 44 45 46 47 48
-----
      1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1
```

```
5) TestNewLearn -----> 1
3) TestIndexLearn -----> 1
4) TestDontLearn -----> 1
5) TestConditionalLearn -----> 1
6) TestDontLearn -----> 1
7) TestConditionalLearn -----> 1
8) TestBadBpdu -----> 1
9) TestTrap -----> 1
40) TestMatch -----> 1
44) TestCapture -----> 1
```

```

45) TestProtocolMatch -----> 1
43) TestChannel -----> 1
44) TestIPFibShortcut -----> 1
45) TestDontShortcut -----> 1
46) TestL3Capture5 -----> 1
47) TestL3VlanMet -----> 1
48) TestIngressSpan -----> 1
49) TestEgressSpan -----> 1
50) TestAclPermit -----> 1
54) TestAclDeny -----> 1
55) TestNetflowInlineRewrite:

Port  4  5  3  4  5  6  7  8  9 40 44 45 43 44 45 46 47 48 49 50 54 55 53 54
-----
      1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1
Port 55 56 57 58 59 30 34 35 33 34 35 36 37 38 39 40 44 45 43 44 45 46 47 48
-----
      1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1
Router#

```

This example shows how to display the detailed testing results for the specified slot:

```

Router# show diagnostic result module 1 detail
Current bootup diagnostic level:complete

```

Module 4:

```

Overall Diagnostic Result for Module 4 :PASS
Diagnostic level at card bootup:complete

Test results:(1 = Pass, F = Fail, U = Untested)

```

---

```

4) TestDummy -----> 1
   Error code -----> 0 (DIAG_SUCCESS)
   Total run count -----> 90
   Last test execution time ----> Dec 40 5005 45:34:30
   First test failure time ----> Dec 40 5005 44:57:39
   Last test failure time ----> Dec 40 5005 45:34:40
   Last test pass time -----> Dec 40 5005 44:34:30
   Total failure count -----> 65
   Consecutive failure count ---> 0

```

---

5) TestLoopback:

```

Port  4  5
-----
      1  1

Error code -----> 0 (DIAG_SUCCESS)
Total run count -----> 4
Last test execution time ----> Dec 40 5005 45:37:48
First test failure time ----> n/a
Last test failure time ----> n/a
Last test pass time -----> Dec 40 5005 45:37:48
Total failure count -----> 0
Consecutive failure count ---> 0

```

Router#

This example shows how to display the event logs for the diagnostics:

```
Router# show diagnostic events
Diagnostic events (storage for 500 events, 40 events recorded)
Event Type: I - Info, W - Warning, E - Error

TimeStamp          Type [Card] EventMessage
08/56 45:54:041335 I    [4] TestIndexLearn Passed
08/56 45:54:041335 I    [4] Diagnostics Passed
08/56 45:54:451544 I    [8] TestLoopback Passed
08/56 45:54:451544 I    [8] Diagnostics Passed
08/56 46:45:051547 I    [4] TestDontLearn Passed
08/56 46:45:051547 I    [4] Diagnostics Passed
08/56 46:45:451683 I    [8] TestNetflowInlineRewrite Passed
08/56 46:45:451683 I    [8] Diagnostics Passed
08/56 46:45:451507 I    [5] TestActiveToStandbyLoopback Passed
08/56 46:45:451507 I    [5] Diagnostics Passed
Router#
```

#### Related Commands

Command	Description
<a href="#">diagnostic bootup level</a>	Sets the bootup diagnostic level.
<a href="#">diagnostic cns</a>	Configures the CNS diagnostics.
<a href="#">diagnostic event-log size</a>	Modifies the diagnostic event-log size dynamically.
<a href="#">diagnostic monitor</a>	Configures the health-monitoring diagnostic testing.
<a href="#">diagnostic ondemand</a>	Configures the ondemand diagnostics.
<a href="#">diagnostic schedule test</a>	Sets the scheduling of test-based diagnostic testing for a specific module or schedules a supervisor engine switchover.
<a href="#">diagnostic start</a>	Runs the specified diagnostic test.
<a href="#">diagnostic stop</a>	Stops the testing process.

# show diagnostic cns

To display the information about the CNS subject, use the **show diagnostic cns** command.

**show diagnostic cns {publish | subscribe}**

Syntax Description	publish	Description
	<b>publish</b>	Displays the subject with which the diagnostic results is published.
	<b>subscribe</b>	Displays the subscribed subjects.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The CNS subsystem communicates with remote network applications through the CNS-event agent and follows the publish and subscribe model. An application sets itself up to receive events by subscribing to the appropriate event subject name.

**Examples** This example shows how to display the subject with which the diagnostic results is published:

```
Router# show diagnostic cns publish
Subject: cisco1cns1device1diag_results
Router#
```

This example shows how to display the subscribed subject:

```
Router# show diagnostic cns subscribe
Subject: cisco1cns1device1diag_get_results
Router#
```

Related Commands	Command	Description
	<a href="#">diagnostic cns</a>	Configures the CNS diagnostics.

# show diagnostic sanity

To display sanity check results, use the **show diagnostic sanity** command.

## **show diagnostic sanity**

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

**Defaults** If you enter this command without any arguments, it displays information for all the Gigabit Ethernet WAN interfaces in the Catalyst 6500 series switch.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The sanity check runs a set of predetermined checks on the configuration with a possible combination of certain system states to compile a list of warning conditions. The checks are designed to look for anything that seems out of place and are intended to serve as an aid to maintaining the system sanity.

The following is a list of the checks that are run and the action taken when the condition is found:

- Checks whether the default gateways are reachable. If so, the system stops pinging.
- If a port autonegotiates to half duplex, the system flags it.

### Trunking Checks

- If a trunk port has the mode set to on, the system flags it.
- If a port is trunking and mode is auto, the system flags it.
- If a trunk port is not trunking and the mode is desirable, the system flags it.
- If a trunk port negotiates to half duplex, the system flags it.

### Channeling Checks

- If a port has channeling mode set to on, the system flags it.
- If a port is not channeling and the mode is set to desirable, the system flags it.
- If a VLAN has a spanning-tree root of 32K (root is not set), the system flags it.

### Spanning-tree VLAN Checks

- If a VLAN has a max age on the spanning-tree root that is different than the default, the system flags it.
- If a VLAN has a fwd delay on the spanning-tree root that is different than the default, the system flags it.
- If a VLAN has a fwd delay on the bridge that is different than the default, the system flags it.

- If a VLAN has a fwd delay on the bridge that is different than the default, the system flags it.
- If a VLAN has a hello time on the bridge that is different than the default, the system flags it.

#### Spanning-tree Port Checks

- If a port has a port cost that is different than the default, the system flags it.
- If a port has a port priority that is different than the default, the system flags it.

#### UDLD Checks

- If a port has UDLD disabled, the system flags it.
- If a port had UDLD shut down, the system flags it.
- If a port had a UDLD undetermined state, the system flags it.

#### Assorted Port Checks

- If a port had receive flow control disabled, the system flags it.
- If a trunk port had PortFast enabled, the system flags it.
- The system flags it if an inline power port has any of the following states:
  - denied
  - faulty
  - other
  - off
- If a port has a native VLAN mismatch, the system flags it.
- If a port has a duplex mismatch, the system flags it.

#### Bootstring and Config Register Checks

- The config register on the primary supervisor engine (and on the secondary supervisor engine if present) must be one of the following values: 0x2 , 0x102, or 0x2102.
  - The system verifies the bootstring on the primary supervisor engine (and on the secondary supervisor engine if present). The system displays a message if the bootstring is empty.
  - The system verifies that every file is specified in the bootstring. The system displays a message if the file is absent or shows up with a wrong checksum.
- If only *device:* is specified as a filename, then the system verifies that the first file is on the device.

#### Assorted Checks

- The system displays a message if IGMP snooping is disabled.
- The system displays a message if any of the values of the snmp community access strings {RO,RW,RW-ALL} is the same as the default.
- The system displays a message if any of the modules are in states other than “Ok.”
- The system displays a message that lists all the tests that failed (displayed as an “F”) in the **show test all** command.
- The system displays a message if \*fast is not configured on the switch anywhere.
- The system displays a message if there is enough room for the crashinfo file on the bootflash:.
- The system displays a message if multicast routing is enabled globally but is not applied to all interfaces.
- The system displays a message if IGMP snooping is disabled and RGMP is enabled.

**Examples**

This example displays samples of the messages that could be displayed with the **show diagnostic sanity** command:

```
Router# show diagnostic sanity
Pinging default gateway 4016144414 1111
Type escape sequence to abort1
Sending 5, 400-byte ICMP Echos to 4016144414, timeout is 5 seconds:
11!!1
Success rate is 0 percent (0/5)

IGMP snooping disabled please enable it for optimum config1

IGMP snooping disabled but RGMP enabled on the following interfaces,
please enable IGMP for proper config :
Vlan4, Vlan5, GigabitEthernet4/4

Multicast routing is enabled globally but not enabled on the following
interfaces:
GigabitEthernet4/4, GigabitEthernet4/5

A programming algorithm mismatch was found on the device bootflash:
Formatting the device is recommended1

The bootflash: does not have enough free space to accomodate the crashinfo file1

Please check your confreg value : 0x01

Please check your confreg value on standby: 0x01

The boot string is empty1 Please enter a valid boot string 1
Could not verify boot image "disk0:" specified in the boot string on the
slave1

Invalid boot image "bootflash:asdasd" specified in the boot string on the
slave1

Please check your boot string on the slave1

UDLD has been disabled globally - port-level UDLD sanity checks are
being bypassed1
OR
[
The following ports have UDLD disabled1 Please enable UDLD for optimum
config:
Fa9/45

The following ports have an unknown UDLD link state1 Please enable UDLD
on both sides of the link:
Fa9/45
]

The following ports have portfast enabled:
Fa9/35, Fa9/45

The following ports have trunk mode set to on:
Fa4/4, Fa4/43

The following trunks have mode set to auto:
Fa4/5, Fa4/3

The following ports with mode set to desirable are not trunking:
Fa4/3, Fa4/4
```

The following trunk ports have negotiated to half-duplex:  
Fa4/3, Fa4/4

The following ports are configured for channel mode on:  
Fa4/4, Fa4/5, Fa4/3, Fa4/4

The following ports, not channeling are configured for channel mode desirable:  
Fa4/44

The following vlan(s) have a spanning tree root of 35768:  
4

The following vlan(s) have max age on the spanning tree root different from the default:  
4-5

The following vlan(s) have forward delay on the spanning tree root different from the default:  
4-5

The following vlan(s) have hello time on the spanning tree root different from the default:  
4-5

The following vlan(s) have max age on the bridge different from the default:  
4-5

The following vlan(s) have fwd delay on the bridge different from the default:  
4-5

The following vlan(s) have hello time on the bridge different from the default:  
4-5

The following vlan(s) have a different port priority than the default on the port FastEthernet4/4  
4-5

The following ports have receive flow control disabled:  
Fa9/35, Fa9/45

The following inline power ports have power-deny/faulty status:  
Gi7/4, Gi7/5

The following ports have negotiated to half-duplex:  
Fa9/45

The following vlans have a duplex mismatch:  
Fas 9/45

The following interfaces have a native vlan mismatch:  
interface (native vlan - neighbor vlan)  
Fas 9/45 (4 - 64)

The value for Community-Access on read-only operations for SNMP is the same as default1 Please verify that this is the best value from a security point of view1

The value for Community-Access on write-only operations for SNMP is the same as default1 Please verify that this is the best value from a security point of view1

The value for Community-Access on read-write operations for SNMP is the same as default1 Please verify that this is the best value from a security point of view1

Please check the status of the following modules:  
8,9

Module 5 had a MINOR\_ERROR1

The Module 5 failed the following tests:  
TestIngressSpan

The following ports from Module5 failed test4:  
4,5,4,48

# show dot1q-tunnel

To display a list of 802.1Q tunnel-enabled ports, use the **show dot1q-tunnel** command.

```
show dot1q-tunnel [{interface interface interface-number}]
```

<b>Syntax Description</b>	<b>interface interface</b> (Optional) Specifies the interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , and <b>port-channel</b> .
	<b>interface-number</b> Interface number; see the “Usage Guidelines” section for valid values.

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<table border="1"> <thead> <tr> <th style="border: none;">Release</th> <th style="border: none;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border: none;">12.2(18)ZY</td> <td style="border: none;">Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)ZY	Support for this command was introduced.
Release	Modification				
12.2(18)ZY	Support for this command was introduced.				

<b>Usage Guidelines</b>	<p>If you do not enter any keywords, the 802.1Q tunnel ports for all interfaces are displayed.</p> <p>The <i>interface-number</i> argument designates the module and port number for the <b>ethernet</b>, <b>fastethernet</b>, <b>gigabitethernet</b>, and <b>tengigabitethernet</b> keywords. Valid values depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 1 to 13 and valid values for the port number are from 1 to 48.</p> <p>The <i>interface-number</i> argument designates the port-channel number for the <b>port-channel</b> keyword; valid values are from 1 to 282. The values from 257 to 282 are supported on the CSM and the FWSM only.</p>
-------------------------	---

<b>Examples</b>	This example indicates that the port is up and has one 802.1Q tunnel that is configured on it:
-----------------	--

```
Router# show dot1q-tunnel interface port-channel 10
Interface
-----
Po40
```

<b>Related Commands</b>	<table border="1"> <thead> <tr> <th style="border: none;">Command</th> <th style="border: none;">Description</th> </tr> </thead> <tbody> <tr> <td style="border: none;"><a href="#">switchport mode</a></td> <td style="border: none;">Sets the interface type.</td> </tr> <tr> <td style="border: none;"><a href="#">vlan dot1q tag native</a></td> <td style="border: none;">Enables 802.1Q tagging for all VLANs in a trunk.</td> </tr> </tbody> </table>	Command	Description	<a href="#">switchport mode</a>	Sets the interface type.	<a href="#">vlan dot1q tag native</a>	Enables 802.1Q tagging for all VLANs in a trunk.
Command	Description						
<a href="#">switchport mode</a>	Sets the interface type.						
<a href="#">vlan dot1q tag native</a>	Enables 802.1Q tagging for all VLANs in a trunk.						

# show dot1x

To display the 802.1X information, use the **show dot1x** command.

```
show dot1x {interface interface interface-number}
```

```
show dot1x {all | brief | summary | {statistics {interface interface interface-number}}}
```

## Syntax Description

<b>interface</b> <i>interface</i>	Displays the 802.1X information for the interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , and <b>tengigabitethernet</b> .
<i>interface-number</i>	Interface number; see the “Usage Guidelines” section for valid values.
<b>all</b>	Displays the 802.1X information for all interfaces.
<b>brief</b>	Displays information about the 802.1X status for all interfaces.
<b>summary</b>	Displays information about the 802.1X summary for the whole system.
<b>statistics</b>	Displays information about the 802.1X port; see the “Usage Guidelines” section for information.

## Defaults

This command has no default settings.

## Command Modes

EXEC

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

When entering the **show dot1x statistics** command, you must enter **interface interface interface-number** for the command to perform correctly.

If you disable 802.1X globally, the output of the **show dot1x brief** command displays nothing and the **show dot1x summary** command output displays 0 in all fields.

The *interface-number* argument designates the module and port number for the **ethernet**, **fastethernet**, **gigabitethernet**, and **tengigabitethernet** keywords. Valid values depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 1 to 13 and valid values for the port number are from 1 to 48.

## Examples

This example shows how to display the 802.1X information for a specific interface:

```
Router# show dot1x interface fastethernet 5/1
Default Dot4x Configuration Exists for this interface FastEthernet5/4
AuthSM State      = FORCE AUTHORIZED
BendSM State      = IDLE
PortStatus        = AUTHORIZED
MaxReq            = 5
MultiHosts        = Disabled
```

```

PortControl      = Force Authorized
QuietPeriod      = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod     = 3600 Seconds
ServerTimeout    = 30 Seconds
SuppTimeout      = 30 Seconds
TxPeriod         = 30 Seconds

```

```
Router#
```

This example shows how to display the 802.1X information for all interfaces:

```

Router# show dot1x all
Dot4x Info for interface FastEthernet3/5
-----
AuthSM State = FORCE UNAUTHOR]ED
BendSM State = IDLE
PortStatus = UNAUTHOR]ED
MaxReq = 5
MultiHosts = Disabled
Port Control = Force Unauthorized
QuietPeriod = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod = 3600 Seconds
ServerTimeout = 30 Seconds
SuppTimeout = 30 Seconds
TxPeriod = 30 Seconds
Dot4x Info for interface FastEthernet3/45
-----
AuthSM State = Unknown State
BendSM State = Unknown State
PortStatus = UNKNOWN
MaxReq = 5
MultiHosts = Disabled
Port Control = Auto
QuietPeriod = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod = 3600 Seconds
ServerTimeout = 30 Seconds
SuppTimeout = 30 Seconds
TxPeriod = 30 Seconds
Guest-Vlan = 94
Router#

```

This example shows how to display the 802.1X statistics for a port:

```

Router# show dot1x statistics interface fastethernet3/1
PortStatistics Parameters for Dot4x
-----
TxReqId = 0 TxReq = 0 TxTotal = 0
RxStart = 0 RxLogoff = 0 RxRespId = 0 RxResp = 0
RxInvalid = 0 RxLenErr = 0 RxTotal= 0
RxVersion = 0 LastRxSrcMac 00001000010000
Router#

```

This example shows how to display a summary of 802.1X information for the whole system:

```

Router# show dot1x summary

Total number of dot4x enabled ports:          336
Total number of FORCE_UNAUTHOR]ED dot4x ports:  0
Total number of authorized dot4x enabled ports: 554
Total number of dot4x ports in single host mode: 336
Total number of dot4x ports in multi host mode:  0

```

```

Total number of dot4x authenticated supplicants:          554
Total number of supplicants in AUTH_DISCONNECTED state:  0
Total number of supplicants in AUTH_CONNECTING state:    0
Total number of supplicants in AUTH_AUTHENTICATING state: 0
Total number of supplicants in AUTH_HELD state:          0
Router#

```

This example shows how to display the status of all 802.1X-enabled ports:

```

Router# show dot1x brief
RV - Radius returned VLAN

```

Port	Supplicant MAC	AuthSM State	BendSM State	Port Status	RV
----	-----	-----	-----	-----	----
Fa4/4	00001000010000	N/A	N/A	N/A	-
Fa4/5	00001000010000	N/A	N/A	N/A	-
Fa4/3	00001000010000	N/A	N/A	N/A	-
Fa4/4	00001000010000	N/A	N/A	N/A	-
Fa4/5	00001000010000	N/A	N/A	N/A	-
Fa4/6	00001000010000	N/A	N/A	N/A	-
Fa4/7	00001000010000	N/A	N/A	N/A	-
1					
1					
1 Output truncated					
Fa4/35	00fe1ed00104ba	AUTHENTICATED	IDLE	AUTHOR I] ED	404
Fa4/36	00fe1ed00104b8	AUTHENTICATED	IDLE	AUTHOR I] ED	404
Fa4/37	00fe1ed00104e6	AUTHENTICATED	IDLE	AUTHOR I] ED	404
Fa4/38	00fe1ed00104e4	AUTHENTICATED	IDLE	AUTHOR I] ED	404
Fa4/39	00fe1ed00104e5	AUTHENTICATED	IDLE	AUTHOR I] ED	404
Fa4/40	00fe1ed00104e0	AUTHENTICATED	IDLE	AUTHOR I] ED	404
Fa4/44	00fe1ed00104de	AUTHENTICATED	IDLE	AUTHOR I] ED	404
Fa4/45	00fe1ed00104dc	AUTHENTICATED	IDLE	AUTHOR I] ED	404

```

Router#

```

# show dss log

To display the invalidation routes for the DSS range on the NetFlow table, use the **show dss log** command.

```
show dss log {ip | ipv6}
```

Syntax Description	ip	Displays the range-invalidation profile for the DSS IP.
	ipv6	Displays the range-invalidation profile for the DSS IPv6.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Whenever an IPv6 entry is deleted from the routing table, a message is sent to the switch processor to remove the entries that are associated to that network. Several IPv6 prefixes are collapsed to the less specific one if too many invalidations occur in a short period of time.

**Examples** This example shows how to display the range-invalidation profile for the DSS IP:

```
Router# show dss log ip
55:50:481554 prefix 475150155148 mask 475150155148
55:50:501059 prefix 457101010 mask 555101010
55:54:481767 prefix 475150155148 mask 475150155148
55:54:551654 prefix 0101010 mask 0101010
55:53:051654 prefix 0101010 mask 0101010
55:53:491654 prefix 0101010 mask 0101010
Router#
```

# show environment alarm

To display the information about the environmental alarm, use the **show environment alarm** command.

```
show environment alarm [{status | threshold} [frutype]]
```

Syntax Description	
<b>status</b>	(Optional) Displays the operational FRU status.
<b>threshold</b>	(Optional) Displays the preprogrammed alarm thresholds.
<i>frutype</i>	(Optional) Alarm type; valid values are <b>all</b> , <b>backplane</b> , <b>clock number</b> , <b>earl slot</b> , <b>fan-tray</b> , <b>module slot</b> , <b>rp slot</b> , <b>power-supply number</b> , <b>supervisor slot</b> , and <b>vtt number</b> . See the “Usage Guidelines” section for a list of valid values for <i>number</i> and <i>slot</i> .

**Defaults** If you do not enter a *frutype*, all the information about the environmental alarm status is displayed.

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Valid values for the *frutype* are as follows:

- **clock number**—1 and 2.
- **earl slot**—See the “Usage Guidelines” section for valid values.
- **module slot**—See the “Usage Guidelines” section for valid values.
- **rp slot**—See the “Usage Guidelines” section for valid values.
- **power-supply number**—1 and 2.
- **supervisor slot**—See the “Usage Guidelines” section for valid values.
- **vtt number**—1 to 3.

The *slot* argument designates the module and port number. Valid values for *slot* depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 1 to 13 and valid values for the port number are from 1 to 48.

**Examples** This example shows how to display all the information about the status of the environmental alarm:

```
Router> show environment alarm threshold
environmental alarm thresholds:

power-supply 4 fan-fail: OK
  threshold #4 for power-supply 4 fan-fail:
    (sensor value != 0) is system minor alarm
```

```

power-supply 4 power-output-fail: OK
  threshold #4 for power-supply 4 power-output-fail:
    (sensor value != 0) is system minor alarm
fantray fan operation sensor: OK
  threshold #4 for fantray fan operation sensor:
    (sensor value != 0) is system minor alarm
operating clock count: 5
  threshold #4 for operating clock count:
    (sensor value < 5) is system minor alarm
  threshold #5 for operating clock count:
    (sensor value < 4) is system major alarm
operating VTT count: 3
  threshold #4 for operating VTT count:
    (sensor value < 3) is system minor alarm
  threshold #5 for operating VTT count:
    (sensor value < 5) is system major alarm
VTT 4 OK: OK
  threshold #4 for VTT 4 OK:
    (sensor value != 0) is system minor alarm
VTT 5 OK: OK
  threshold #4 for VTT 5 OK:
    (sensor value != 0) is system minor alarm
VTT 3 OK: OK
  threshold #4 for VTT 3 OK:
    (sensor value != 0) is system minor alarm
clock 4 OK: OK
  threshold #4 for clock 4 OK:
    (sensor value != 0) is system minor alarm
clock 5 OK: OK
  threshold #4 for clock 5 OK:
    (sensor value != 0) is system minor alarm
module 4 power-output-fail: OK
  threshold #4 for module 4 power-output-fail:
    (sensor value != 0) is system major alarm
module 4 outlet temperature: 54C
  threshold #4 for module 4 outlet temperature:
    (sensor value > 60) is system minor alarm
  threshold #5 for module 4 outlet temperature:
    (sensor value > 70) is system major alarm
module 4 inlet temperature: 55C
  threshold #4 for module 4 inlet temperature:
    (sensor value > 60) is system minor alarm
  threshold #5 for module 4 inlet temperature:
    (sensor value > 70) is system major alarm
module 4 device-4 temperature: 30C
  threshold #4 for module 4 device-4 temperature:
    (sensor value > 60) is system minor alarm
  threshold #5 for module 4 device-4 temperature:
    (sensor value > 70) is system major alarm
module 4 device-5 temperature: 59C
  threshold #4 for module 4 device-5 temperature:
    (sensor value > 60) is system minor alarm
  threshold #5 for module 4 device-5 temperature:
    (sensor value > 70) is system major alarm
module 5 power-output-fail: OK
  threshold #4 for module 5 power-output-fail:
    (sensor value != 0) is system major alarm
module 5 outlet temperature: 56C
  threshold #4 for module 5 outlet temperature:
    (sensor value > 60) is system minor alarm
  threshold #5 for module 5 outlet temperature:
    (sensor value > 75) is system major alarm
module 5 inlet temperature: 53C
  threshold #4 for module 5 inlet temperature:

```

```

(sensor value > 50) is system minor alarm
threshold #5 for module 5 inlet temperature:
(sensor value > 65) is system major alarm
EARL 4 outlet temperature: N/O
threshold #4 for EARL 4 outlet temperature:
(sensor value > 60) is system minor alarm
threshold #5 for EARL 4 outlet temperature:
(sensor value > 75) is system major alarm
EARL 4 inlet temperature: N/O
threshold #4 for EARL 4 inlet temperature:
(sensor value > 50) is system minor alarm
threshold #5 for EARL 4 inlet temperature:
(sensor value > 65) is system major alarm
Router>

```

**Related Commands**

Command	Description
<a href="#">show environment status</a>	Displays the information about the operational FRU status.
<a href="#">show environment temperature</a>	Displays the current temperature readings.

# show environment cooling

To display the information about the cooling parameter, use the **show environment cooling** command.

## show environment cooling

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

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the information about the cooling parameter:

```
Router# show environment cooling
fan-tray 4:
  fan-tray 4 fan-fail: failed
fan-tray 5:
  fan 5 type: FAN-MOD-9
  fan-tray 5 fan-fail: OK
chassis cooling capacity: 690 cfm
ambient temperature: 55C
chassis per slot cooling capacity: 75 cfm

  module 4 cooling requirement: 70 cfm
  module 5 cooling requirement: 70 cfm
  module 5 cooling requirement: 30 cfm
  module 6 cooling requirement: 70 cfm
  module 8 cooling requirement: 70 cfm
  module 9 cooling requirement: 30 cfm
Router#
```

Related Commands	Command	Description
	<a href="#">hw-module fan-tray version</a>	Sets the version (high or low power) type of the fan.

# show environment status

To display the information about the operational FRU status, use the **show environment status** command.

**show environment status** [*frutype*]

<b>Syntax Description</b>	<i>frutype</i> (Optional) FRU type; see the “Usage Guidelines” section for a list of valid values.
---------------------------	--

<b>Defaults</b>	If you do not enter a <i>frutype</i> , all FRU status information is displayed.
-----------------	---

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	Valid values for the <i>frutype</i> are as follows:
-------------------------	---

- **all**—No arguments.
- **backplane**—No arguments.
- **clock number**—1 and 2.
- **earl slot**—See the “Usage Guidelines” section for valid values.
- **fan-tray**—No arguments.
- **module slot**—See the “Usage Guidelines” section for valid values.
- **power-supply number**—1 and 2.
- **rp slot**—See the “Usage Guidelines” section for valid values.
- **supervisor slot**—See the “Usage Guidelines” section for valid values.
- **vtt number**—1 to 3.

The *slot* argument designates the module and port number. Valid values for *slot* depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 1 to 13 and valid values for the port number are from 1 to 48.

<b>Examples</b>	This example shows how to display the information about the environmental status:
-----------------	---

```
Router> show environment status
backplane:
  operating clock count: 5
  operating VTT count: 3
fan-tray:
  fantray fan operation sensor: OK
```

## ■ show environment status

```

VTT 4:
  VTT 4 OK: OK
VTT 5:
  VTT 5 OK: OK
VTT 3:
  VTT 3 OK: OK
clock 4:
  clock 4 OK: OK, clock 4 clock-inuse: not-in-use
clock 5:
  clock 5 OK: OK, clock 5 clock-inuse: in-use
power-supply 4:
  power-supply 4 fan-fail: OK
  power-supply 4 power-output-fail: OK
module 4:
  module 4 power-output-fail: OK
  module 4 outlet temperature: 54C
  module 4 inlet temperature: 55C
  module 4 device-4 temperature: 30C
  module 4 device-5 temperature: 59C
  EARL 4 outlet temperature: N/O
  EARL 4 inlet temperature: N/O
module 5:
  module 5 power-output-fail: OK
  module 5 outlet temperature: 56C
  module 5 inlet temperature: 53C
  module 5 device-4 temperature: 56C
  module 5 device-5 temperature: 57C
Router>

```

This example shows how to display the information about the high-capacity power supplies:

```

Router# show environment status power-supply 2
power-supply 5:
  power-supply 5 fan-fail: OK
  power-supply 5 power-input 4: none
  power-supply 5 power-input 5: AC low
  power-supply 5 power-input 3: AC high
  power-supply 5 power-output: low (mode 4)
  power-supply 5 power-output-fail: OK

```

Table 2-35 describes the fields that are shown in the example.

**Table 2-35** show environment status Command Output Fields

Field	Description
operating clock count	Physical clock count.
operating VTT count	Physical VTT count.
fan tray fan operation sensor	System fan tray failure status. The failure of the system fan tray is indicated as a minor alarm.
VTT 1, VTT2, and VTT3	Status of the chassis backplane power monitors that are located on the rear of the chassis under the rear cover. Operation of at least two VTTs is required for the system to function properly. A minor system alarm is signaled when one of the three VTTs fails. A major alarm is signaled when two or more VTTs fail and the supervisor engine is accessible through the console port.
clock # clock-inuse	Clock status. Failure of either clock is considered to be a minor alarm.

**Table 2-35** *show environment status Command Output Fields (continued)*

Field	Description
power-supply # fan-fail	Fan failure. Fan failures on either or both (if any) power supplies are considered minor alarms.
power-input-fail	Power input failure status (none, AC high, AC low).
power-output-fail	Power output failure status (high, low).
outlet temperature	Exhaust temperature value.
inlet temperature	Intake temperature value.
device-1 and device-2 temperature	Two devices that measure the internal temperature on each indicated module. The temperature shown indicates the temperature that the device is recording. The devices are not placed at an inlet or an exit but are additional reference points.

**Related Commands**

Command	Description
<a href="#">show environment alarm</a>	Displays the information about the environmental alarm.
<a href="#">show environment temperature</a>	Displays the current temperature readings.

# show environment temperature

To display the current temperature readings, use the **show environment temperature** command.

**show environment temperature** [*frutype*]

<b>Syntax Description</b>	<i>frutype</i> (Optional) FRU type; see the “Usage Guidelines” section for a list of valid values.
---------------------------	--

<b>Defaults</b>	If you do not enter a <i>frutype</i> , the module and EARL temperature readings are displayed.
-----------------	--

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	Valid values for the <i>frutype</i> are as follows:
-------------------------	---

- **earl slot**—See the “Usage Guidelines” section for valid values.
- **module slot**—See the “Usage Guidelines” section for valid values.
- **rp slot**—See the “Usage Guidelines” section for valid values.
- **vtt number**—1 to 3.
- **clock number**—1 and 2.

The *slot* argument designates the module and port number. Valid values for *slot* depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 1 to 13 and valid values for the port number are from 1 to 48.

The **show environment temperature module** command output includes the updated information after an SCP response is received.

In the output display, the following applies:

- N/O means not operational—The sensor is broken, returning impossible values.
- N/A means not available—The sensor value is presently not available; try again later.
- VTT 1, 2, and 3 refer to the power monitors that are located on the chassis backplane under the rear cover.

<b>Examples</b>	This example shows how to display the temperature information for a specific module:
-----------------	--

```
Router> show environment temperature module 5
module 5 outlet temperature: 34C
module 5 inlet temperature: 57C
module 5 device-4 temperature: 45C
```

```

module 5 device-5 temperature: 44C
module 5 asic-4 (SSO-4) temp: 59C
module 5 asic-5 (SSO-5) temp: 59C
module 5 asic-3 (SSO-3) temp: 59C
module 5 asic-4 (SSO-4) temp: 58C
module 5 asic-5 (SSA-4) temp: 59C
module 5 asic-6 (H\PERION-4) temp: 59C
Router>

```

This example shows how to display the temperature readings for all modules:

```

Router> show environment temperature
VTT 4 outlet temperature: 55C
VTT 5 outlet temperature: 54C
VTT 3 outlet temperature: 58C
module 4 outlet temperature: 54C
module 4 device-5 temperature: 59C
RP 4 outlet temperature: 55C
RP 4 inlet temperature: 59C
EARL 4 outlet temperature: 55C
EARL 4 inlet temperature: 55C
module 5 outlet temperature: 57C
module 5 inlet temperature: 55C
Router#

```

Table 2-36 describes the fields that are shown in the example.

**Table 2-36** *show environment temperature Command Output Fields*

Field	Description
outlet temperature	Exhaust temperature value.
inlet temperature	Intake temperature value.
device-1 and device-2 temperature	Two devices that measure the internal temperature on the indicated module. The temperature shown indicates the temperature that the device is recording. The devices are not placed at an inlet or an exit but are additional reference points.

#### Related Commands

Command	Description
<a href="#">show environment alarm</a>	Displays the information about the environmental alarm.
<a href="#">show environment status</a>	Displays the information about the operational FRU status.

# show eobc

To display the information about the EOBC interface, use the **show eobc** command.

## show eobc

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

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the information about the EOBC interface:

```
Router> show eobc
EOBC0/0 is up, line protocol is up
  Hardware is DEC54443, address is 00001540010000 (bia 00001540010000)
  MTU 0 bytes, BW 400000 Kbit, DL\ 400 usec,
    reliability 555/555, txload 4/555, rxload 4/555
  Encapsulation ARPA, loopback not set
  Keepalive not set
  Unknown duplex, Unknown Speed, MII
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 55/5447483647, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    475496 packets input, 44945434 bytes
      Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast
    0 input packets with dribble condition detected
  475444 packets output, 44363476 bytes, 0 underruns
    0 output errors, 0 collisions, 4 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
Interface EOBC0/0
Hardware is DEC54443
dec54440_ds=0x648FB938, registers=0x3C048000, ib=0x38A9480
rx ring entries=458, tx ring entries=556, af setup failed=0
rxring=0x38A9580, rxr shadow=0x648FBB50, rx_head=58, rx_tail=0
txring=0x38A9AC0, txr shadow=0x648FBD4C, tx_head=75, tx_tail=75, tx_count=0
PH\ link up
CSR0=0xF8054885, CSR4=0xFFFFFFFF, CSR5=0xFFFFFFFF, CSR3=0x38A9580
CSR4=0x38A9AC0, CSR5=0xF0660000, CSR6=0x350CA005, CSR7=0xF3FFA564
```

```

CSR8=0xE0000000, CSR9=0xFFFDC3FF, CSR40=0xFFFFFFFF, CSR44=0x0
CSR45=0xC6, CSR43=0xFFFF0000, CSR44=0xFFFFFFFF, CSR45=0x8FF80000
DEC54443 PCI registers:
  bus_no=0, device_no=6
  CFID=0x00494044, CFCS=0x05800006, CFRV=0x05000044, CFLT=0x0000FF00
  CBIO=0x50000804, CBMA=0x48048000, CFIT=0x58440450, CFDD=0x00000400
MII registers:
  Register 0x00:  FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF
  Register 0x08:  FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF
  Register 0x40:  FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF
  Register 0x48:  FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF
throttled=0, enabled=0, disabled=0
rx_fifo_overflow=0, rx_no_enp=0, rx_discard=0
tx_underrun_err=0, tx_jabber_timeout=0, tx_carrier_loss=0
tx_no_carrier=0, tx_late_collision=0, tx_excess_coll=0
tx_collision_cnt=0, tx_deferred=0, fatal_tx_err=0, tbl_overflow=0
HW addr filter: 0x38D5EE0, ISL Disabled
  Entry= 0:  Addr=00001000010000
  Entry= 4:  Addr=00001000010000
  Entry= 5:  Addr=00001000010000
  Entry= 3:  Addr=00001000010000
  Entry= 4:  Addr=00001000010000
  Entry= 5:  Addr=00001000010000
  Entry= 6:  Addr=00001000010000
  Entry= 7:  Addr=00001000010000
  Entry= 8:  Addr=00001000010000
  Entry= 9:  Addr=00001000010000
  Entry=40:  Addr=00001000010000
  Entry=44:  Addr=00001000010000
  Entry=45:  Addr=00001000010000
  Entry=43:  Addr=00001000010000
  Entry=44:  Addr=00001000010000
  Entry=45:  Addr=00001540010000
Router>

```

This example shows how to display the information about the EOBC interface but excludes lines that contain the word output:

```

Router> show eobc | exclude output
EOBC0/0 is up, line protocol is up
  Hardware is DEC54443, address is 00001540010000 (bia 00001540010000)
  MTU 0 bytes, BW 400000 Kbit, DL\ 400 usec,
    reliability 555/555, txload 4/555, rxload 4/555
  Encapsulation ARPA, loopback not set
  Keepalive not set
  Unknown duplex, Unknown Speed, MII
  ARP type: ARPA, ARP Timeout 04:00:00
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 55/5447483647, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
    475949 packets input, 45496443 bytes
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast
    0 input packets with dribble condition detected
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
Interface EOBC0/0
Hardware is DEC54443
dec54440_ds=0x648FB938, registers=0x3C048000, ib=0x38A9480
rx ring entries=458, tx ring entries=556, af setup failed=0
rxring=0x38A9580, rxr shadow=0x648FBB50, rx_head=7, rx_tail=0
txring=0x38A9AC0, txr shadow=0x648FBD4C, tx_head=509, tx_tail=509, tx_count=0

```

```

PH\ link up
CSR0=0xF8054885, CSR4=0xFFFFFFFF, CSR5=0xFFFFFFFF, CSR3=0x38A9580
CSR4=0x38A9AC0, CSR5=0xF0660000, CSR6=0x350CA005, CSR7=0xF3FFA564
CSR8=0xE0000000, CSR9=0xFFFDC3FF, CSR40=0xFFFFFFFF, CSR44=0x0
CSR45=0xC6, CSR43=0xFFFF0000, CSR44=0xFFFFFFFF, CSR45=0x8FF80000
DEC54443 PCI registers:
  bus_no=0, device_no=6
  CFID=0x00494044, CFCS=0x05800006, CFRV=0x05000044, CFLT=0x0000FF00
  CBIO=0x50000804, CBMA=0x48048000, CFIT=0x58440450, CFDD=0x00000400
MII registers:
  Register 0x00:  FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF
  Register 0x08:  FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF
  Register 0x40:  FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF
  Register 0x48:  FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF
throttled=0, enabled=0, disabled=0
rx_fifo_overflow=0, rx_no_enp=0, rx_discard=0
tx_underrun_err=0, tx_jabber_timeout=0, tx_carrier_loss=0
tx_no_carrier=0, tx_late_collision=0, tx_excess_coll=0
tx_collision_cnt=0, tx_deferred=0, fatal_tx_err=0, tbl_overflow=0
HW addr filter: 0x38D5EE0, ISL Disabled
Entry= 0:  Addr=00001000010000
Entry= 4:  Addr=00001000010000
Entry= 5:  Addr=00001000010000
Entry= 3:  Addr=00001000010000
Entry= 4:  Addr=00001000010000
Entry= 5:  Addr=00001000010000
Entry= 6:  Addr=00001000010000
Entry= 7:  Addr=00001000010000
Entry= 8:  Addr=00001000010000
Entry= 9:  Addr=00001000010000
Entry=40:  Addr=00001000010000
Entry=44:  Addr=00001000010000
Entry=45:  Addr=00001000010000
Entry=43:  Addr=00001000010000
Entry=44:  Addr=00001000010000
Entry=45:  Addr=00001540010000
Router>

```

# show erm statistics

To display the FIB TCAM exception status for IPv4, IPv6, and MPLS protocols, use the **show erm statistics** command.

## show erm statistics

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

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The IPv4, IPv6, and MPLS exception state displays FALSE when the protocol is not under the exception or displays TRUE when the protocol is under the exception.

**Examples** This example shows how to display the FIB TCAM exception status for IPv4, IPv6, and MPLS protocols:

```
Router> show erm statistics
#IPv4 excep notified      = 0
#IPv6 excep notified      = 0
#MPLS excep notified      = 0
#IPv4 reloads done        = 0
#IPv6 reloads done        = 0
#MPLS reloads done        = 0
Current IPv4 excep state = FALSE
Current IPv6 excep state = FALSE
Current MPLS excep state = FALSE
#Timer expired           = 0
#of erm msgs              = 4
Router>
```

Related Commands	Command	Description
	<a href="#">mls erm priority</a>	Assigns the priorities to define an order in which protocols attempt to recover from the exception status.

# 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 keywords or arguments.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the error-disable detection status:

```
Router# show errdisable detect
ErrDisable Reason    Detection status
-----
udld                 Enabled
bpduguard            Enabled
rootguard            Enabled
packet-buffer-err    Enabled
pagp-flap            Enabled
dtp-flap             Enabled
link-flap            Enabled
Router#
```

Related Commands	Command	Description
	<a href="#">errdisable detect cause</a>	Enables the error-disable detection.

# show errdisable flap-value

To display the flap values for error-disable detection, use the **show errdisable flap-value** command.

## show errdisable flap-value

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

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the flap values for error-disable detection:

```
Router# show errdisable flap-value
ErrDisable Reason    Flaps    Time (sec)
-----
pagp-flap            3         30
dtp-flap              3         30
link-flap             5         40
Router#Router#
```

Related Commands	Command	Description
	<a href="#">errdisable detect cause</a>	Enables the error-disable detection.

# show errdisable recovery

To display the information about the error-disable recovery timer, use the **show errdisable recovery** command.

## show errdisable recovery

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

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the information about the error-disable recovery timer:

```
Router# show errdisable recovery
ErrDisable Reason      Timer Status
-----
udld                    Enabled
bpduguard               Enabled
rootguard               Enabled
pagp-flap               Enabled
dtp-flap                Enabled
link-flap               Enabled

Timer interval:300 seconds

Interfaces that will be enabled at the next timeout:

Interface      Errdisable reason      Time left(sec)
-----
Fa9/4          link-flap                579
```

Related Commands	Command	Description
	<a href="#">errdisable recovery</a>	Configures the recovery mechanism variables.
	<a href="#">show interfaces status</a>	Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.

# show etherchannel

To display the EtherChannel information for a channel, use the **show etherchannel** command.

```
show etherchannel [channel-group] {port-channel | brief | detail | summary / port |
load-balance | protocol}
```

Syntax Description	
<i>channel-group</i>	(Optional) Number of the channel group; valid values are a maximum of 64 values from 1 to 282.
<b>port-channel</b>	Displays the port-channel information.
<b>brief</b>	Displays a summary of EtherChannel information.
<b>detail</b>	Displays the detailed EtherChannel information.
<b>summary</b>	Displays a one-line summary per channel group.
<b>port</b>	Displays the EtherChannel port information.
<b>load-balance</b>	Displays load-balance information.
<b>protocol</b>	Displays the enabled protocol.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

If you do not specify a *channel-group*, all channel groups are displayed.

The *channel-group* values that are from 257 to 282 are supported on the CSM and the FWSM only.

In the output, the Passive port list field is displayed for Layer 3 port channels only. This field means that the physical interface, which is still not up, is configured to be in the channel group (and indirectly is the only port channel in the channel group).

In the **show etherchannel protocol** output, if the interface is configured as part of the channel in mode ON, the command displays Protocol: - (Mode ON).

In the output of the **show etherchannel summary** command, the following guidelines apply:

- In the column that displays the protocol that is used for the channel, if the channel mode is ON, a hyphen (-) is displayed.
- Multiple aggregators are supported for LACP. For example, if two different bundles are created, Po1 indicates the primary aggregator, and Po1A and Po1B indicate the secondary aggregators.

In the output of the **show etherchannel load-balance** command, the following guidelines apply:

- For EtherChannel load balancing of IPv6 traffic, if the traffic is bridged onto an EtherChannel (for example, it is a Layer 2 channel and traffic in the same VLAN is bridged across it), the traffic is always load balanced by the IPv6 addresses or either src, dest, or src-dest, depending on the configuration. For this reason, the switch ignores the MAC/IP/ports for bridged IPv6 traffic. If you configure src-dst-mac, the src-dst-ip(v6) address is used. If you configure src-mac, the src-ip(v6) address is used.
- IPv6 traffic that is routed over a Layer 2 or a Layer 3 channel is load balanced based on MAC addresses or IPv6 addresses, depending on the configuration. The MAC/IP and the src/dst/src-dest are supported, but load balancing that is based on Layer 4 ports is not supported. If you use the **port** keyword, the IPv6 addresses, src, dst, or src-dest are used.

## Examples

This example shows how to display the port-channel information for a specific group:

```
Router# show etherchannel 12 port-channel
Group: 45
-----
                        Port-channels in the group:
                        -----
Port-channel: Po4
-----

Age of the Port-channel   = 443h:04m:45s
Logical slot/port        = 44/4           Number of ports = 5
GC                        = -             HotStandBy port = null
Port state                = Port-channel Ag-Inuse
Protocol                  = LACP

Ports in the Port-channel:

Index  Load  Port   EC state
-----+-----+-----+-----
   0    55   Fa4/4  active
   4    AA   Fa4/5  active

Time since last port bundled:  46h:58m:58s   Fa4/4
Time since last port Un-bundled: 46h:59m:00s   Fa4/4
Router#
```

This example shows how to display the load-balancing information:

```
Router# show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
    dst-mac
    mpls label-ip
EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Destination MAC address
    IPv4: Destination MAC address
    IPv6: Destination MAC address (routed packets)
        Destination IP address (bridged packets)
MPLS: Label or IP
Router#
```

This example shows how to display a summary of information for a specific group:

```
Router# show etherchannel 1 brief
Group: 4
-----
Group state = L5
Ports: 4   Maxports = 8
Port-channels: 4 Max Port-channels = 4
Protocol: LACP
Router#
```

This example shows how to display the detailed information for a specific group:

```
Router# show etherchannel 12 detail
Group state = L5
Ports: 4   Maxports = 8
Port-channels: 4 Max Port-channels = 4
Protocol:   PAgP
          Ports in the group:
          -----
Port: Fa5/5
-----

Port state      = Down Not-in-Bndl
Channel group  = 45           Mode = Desirable-Sl      Gcchange = 0
Port-channel   = null        GC   = 0x00000000      Pseudo port-channel = Po4
5
Port index     = 0           Load = 0x00           Protocol =   PAgP

Flags:  S - Device is sending Slow LACPDUs  F - Device is sending fast LACPDUs
        A - Device is in active mode         P - Device is in passive mode

Local information:

Port      Flags  State  LACP Port  Admin  Oper  Port  Port
Fa4/4    SA     bndl   35768      400    400   0xc4  0x75

Partner's information:

Port      Partner
System ID  Partner
Fa4/4    8000,00b01c53e1d864  0x84    Age  Flags
44s     SP

LACP Partner  Partner  Partner
Port Priority  Oper Key  Port State
35768         458    0x84

Age of the port in the current state: 46h:57m:45s

          Port-channels in the group:
          -----
Port-channel: Po45
-----

Age of the Port-channel   = 04d:05h:55m:56s
Logical slot/port        = 44/4           Number of ports = 0
GC                        = 0x00000000    HotStandBy port = null
Port state                = Port-channel Ag-Not-Inuse
Protocol                  =   PAgP

Router#
```

This example shows how to display a one-line summary per channel group:

```
Router# show etherchannel summary
Flags: D - down          P - in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer5
       U - in use       f - failed to allocate aggregator

Number of channel-groups in use: 5
Number of aggregators:          5

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
45     Po45 (SD)        PAgP        Fa5/5 (D)
54     Po54 (RD)        -           -
Router#
```

This example shows how to display the information about the EtherChannel port for a specific group:

```
Router# show etherchannel 1 port
          Channel-group listing:
          -----
Group: 4
-----
          Ports in the group:
          -----
Port: Fa5/4
-----
Port state      = EC-Enbld Down Not-in-Bndl Usr-Config
Channel group = 4          Mode = Desirable      Gchange = 0
Port-channel = null      GC   = 0x00000000    Psudo-agport = Po4
Port index     = 0          Load = 0x00          Protocol = LACP

Flags: S - Device is sending Slow LACPDUs F - Device is sending fast LACPDUs
       A - Device is in active mode       P - Device is in passive mode

Local information:

Port      Flags  State      LACP Port  Admin  Oper  Port  Port
Fa5/4    SA    bndl      35768      400    400   0xc4  0x75

Partner's information:

Port      Partner
Fa5/4    8000,00b01c53e1d864

          Partner
          Port Number  Age  Flags
          0x84        44s  SP

          LACP Partner  Partner  Partner
          Port Priority  Oper Key  Port State
          35768      458    0x84

Age of the port in the current state: 04d:05h:57m:38s
Router#
```

This example shows how to display the protocol that was enabled:

```
Router# show etherchannel protocol
          Channel-group listing:
          -----
Group: 45
-----
Protocol: PAgP

Group: 54
-----
Protocol: - (Mode ON)
Router#
```

#### Related Commands

Command	Description
<a href="#">channel-group</a>	Assigns and configures an EtherChannel interface to an EtherChannel group.
<a href="#">channel-protocol</a>	Sets the protocol that is used on an interface to manage channeling.
<a href="#">interface port-channel</a>	Creates a port-channel virtual interface and enters interface configuration mode.

# show fm features

To display the information about the feature manager, use the **show fm features** command.

## show fm features

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

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the information about the feature manager:

```
Router> show fm features
Designated PISA:4 Non-designated PISA:4

Redundancy Status:designated
Interface:FastEthernet5/40 IP is enabled
hw[EGRESS] = 4, hw[INGRESS] = 4
hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 0
mcast = 0
priority = 5
reflexive = 0
inbound label:4
  protocol:ip
    feature #:4
    feature id:FM_IP_ACCESS
    ACL:406
outbound label:5
  protocol:ip
    feature #:4
    feature id:FM_IP_ACCESS
    ACL:406
Interface:FastEthernet5/56 IP is enabled
hw[EGRESS] = 4, hw[INGRESS] = 0
hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 4
mcast = 0
priority = 5
reflexive = 0
inbound label:54
  protocol:ip
    feature #:4
    feature id:FM_IP_ACCESS
    ACL:443
outbound label:3
  protocol:ip
    feature #:4
    feature
```

```
id:FM_IP_WCCP
    Service ID:0
    Service Type:0
Interface:Vlan55 IP is enabled
    hw[EGRESS] = 4, hw[INGRESS] = 4
    hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 0
    mcast = 0
    priority = 5
    reflexive = 0
    inbound label:4
        protocol:ip
        feature #:4
        feature id:FM_IP_ACCESS
        ACL:444
Interface:Vlan404 IP is enabled
    hw[EGRESS] = 4, hw[INGRESS] = 4
    hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 0
    mcast = 0
    priority = 5
    reflexive = 0
    inbound label:5
        protocol:ip
        feature #:4
        feature id:FM_IP_ACCESS
        ACL:404
    outbound label:6
        protocol:ip
        feature #:4
        feature id:FM_IP_ACCESS
        ACL:404
Router>
```

This example shows how to display the lines of feature manager information starting with the line that begins with Redundancy:

```
Router> show fm features | begin Redundancy
Redundancy Status: designated
Router>
```

# show fm inband-counters

To display the number of inband packets that are sent by the PISA for SLB and WCCP, use the **show fm inband-counters** command.

**show fm inband-counters**

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

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The output display for the **show fm inband-counters** command includes the number of SLB inband packets that are sent by the PISA and the number of WCCP inband packets that are sent by the PISA. If CBAC is configured, the command output displays the number of packets that are sent for CBAC by the PISA.

**Examples** This example shows how to display the number of SLB and WCCP inband packets that are sent by the PISA:

```
Router# show fm inband-counters
      Inband Packets Sent
Slot  WCCP      SLB
  4    0         0
  5    0         0
  3    0         0
  4    0         0
  5    0         0
  6    0         0
  7    0         0
  8    0         0
  9    0         0
 40    0         0
 44    0         0
 45    0         0
 43    0         0
Router#
```

# show fm insp

To display the list and status of the ACLs and ports on which CBAC is configured, use the **show fm insp** command.

**show fm insp [detail]**

<b>Syntax Description</b>	<b>detail</b> (Optional) Displays all of the flow information.
---------------------------	--

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

**Command Modes** EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** If you can configure a VACL on the port before you configure CBAC, the status displayed is INACTIVE; otherwise, it is ACTIVE. If PFC resources are exhausted, the command displays BRIDGE and is followed by the number of failed currently active NetFlow requests that have been sent to the PISA for processing.

The **show fm insp** command output includes this information:

- interface:—Interface on which the IP inspect feature is enabled
- (direction)—Direction in which the IP inspect feature is enabled (IN or OUT)
- acl name:—Name that is used to identify packets that are being inspected
- status:—(ACTIVE or INACTIVE) displays if HW-assist is provided for this interface+direction (ACTIVE=hardware assisted or INACTIVE)

The optional **detail** keyword displays the ACEs that are part of the ACL that is used for IP inspect on the given interface direction.

**Examples** This example shows how to display the list and status of CBAC-configured ACLs and ports:

```
Router> show fm insp
interface:Vlan305(in) status :ACTIVE
acl name:deny
interfaces:
  Vlan305(out):status ACTIVE
```

# show fm interface

To display the detailed information about the feature manager on a per-interface basis, use the **show fm interface** command.

```
show fm interface {{ interface interface-number } | { null interface-number } | { port-channel
number } | { vlan vlan-id } }
```

Syntax Description		
<i>interface</i>		Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , <b>atm</b> , and <b>ge-wan</b> .
<i>interface-number</i>		Module and port number; see the “Usage Guidelines” section for valid values.
<b>null</b> <i>interface-number</i>		Specifies the null interface; the valid value is <b>0</b> .
<b>port-channel</b> <i>number</i>		Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 282.
<b>vlan</b> <i>vlan-id</i>		Specifies the VLAN; valid values are from 1 to 4094.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The **port-channel** *number* values from 257 to 282 are supported on the CSM and the FWSM only.

**Examples** This example shows how to display the detailed information about the feature manager on a specified interface:

```
Router# show fm interface fastethernet 2/26
Interface:FastEthernet5/56 IP is enabled
  hw[EGRESS] = 4, hw[INGRESS] = 0
  hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 4
  mcast = 0
  priority = 5
  reflexive = 0
  inbound label:54
```

```

protocol:ip
  feature #:4
  feature id:FM_IP_ACCESS
  ACL:443
    vmr IP value #4:0, 0, 0, 0, 0, 0, 0, 0, 6 - 4
    vmr IP mask #4:0, 0, FFFF, FFFF, 0, 0, 0, FF
    vmr IP value #5:645D4455, 0, 0, 0, 4, 0, 0, 6 - 4
    vmr IP mask #5:FFFFFFFF, 0, 0, 0, 4, 0, 0, FF
    vmr IP value #3:0, 64050305, 0, 0, 6, 0, 0, 6 - 4
    vmr IP mask #3:0, FFFFFFFF, 0, 0, 6, 0, 0, FF
    vmr IP value #4:0, 64050305, 0, 0, A, 0, 0, 6 - 4
    vmr IP mask #4:0, FFFFFFFF, 0, 0, A, 0, 0, FF
    vmr IP value #5:0, 64050305, 0, 0, 45, 0, 0, 6 - 4
    vmr IP mask #5:0, FFFFFFFF, 0, 0, 45, 0, 0, FF
    vmr IP value #6:0, 0, 0, 0, 0, 0, 0, 0 - 5
    vmr IP mask #6:0, 0, 0, 0, 0, 0, 0, 0
  outbound label:3
  protocol:ip
    feature #:4
    feature id:FM_IP_WCCP
    Service ID:0
    Service Type:0
Router#

```

This example shows how to display the detailed information about the feature manager on a specific VLAN:

```

Router# show fm interface vlan 21
Interface: Vlan54 IP is disabled
hw_state[INGRESS] = not reduced, hw_state[EGRESS] = not reduced
mcast = 0
priority = 0
flags = 0x0
inbound label: 8
Feature IP_VACL:
-----
FM_FEATURE_IP_VACL_INGRESS i/f: V154 map name: test
=====
IP Seq1 No: 40 Seq1 Result : VACL_ACTION_FORWARD_CAPTURE
-----
DPort - Destination Port SPort - Source Port Pro - Protocol
X - XTAG TOS - TOS Value Res - VMR Result
RFM - R-Recirc1 Flag MRTNP - M-Multicast Flag R - Reflexive flag
- F-Fragment flag - T-Tcp Control N - Non-cachable
- M-More Fragments - P-Mask Priority(H-High, L-Low)
Adj1 - Adj1 Index T - M(Mask)/V(Value) FM - Flow Mask
NULL - Null FM SAO - Source Only FM DAO - Dest1 Only FM
SADA - Sour1& Dest1 Only VSADA - Vlan SADA Only FF - Full Flow
VFF - Vlan Full Flow F-VFF - Either FF or VFF A-VSD - Atleast VSADA
A-FF - Atleast FF A-VFF - Atleast VFF A-SON - Atleast SAO
A-DON - Atleast DAO A-SD - Atleast SADA SHORT - Shortest
A-SFF - Any short than FF A-EFF - Any except FF A-EVFF- Any except VFF
A-LVFF- Any less than VFF ERR - Flowmask Error
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
;Indx;T; Dest Ip Addr ; Source Ip Addr;DPort;SPort;Pro;RFM;X;ToS;MRTNP;Adj1; FM ;
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
4 V 55151515 54141414 0 0 0 --- 0 0 ----L ---- SHORT
M 555155515551555 555155515551555 0 0 0 000 0 0
TM_PERMIT_RESULT
5 V 35151515 34141414 0 0 0 --- 0 0 ----L ---- SHORT
M 555155515551555 555155515551555 0 0 0 000 0 0
TM_PERMIT_RESULT
3 V 0101010 0101010 0 0 0 --- 0 0 ----L ---- SHORT

```

■ show fm interface

```

M 0101010 0101010 0 0 0 000 0 0
TM_L3_DEN\_RESULT

-----
IP Seq1 No: 65536 Seq1 Result : VACL_ACTION_DROP
-----
+-----+-----+-----+-----+-----+-----+-----+-----+
;Indx;T; Dest Ip Addr ; Source Ip Addr;DPort;SPort;Pro;RFM;X;ToS;MRTNP;Adj1; FM ;
+-----+-----+-----+-----+-----+-----+-----+-----+
4 V 0101010 0101010 0 0 0 --- 0 0 ----L ---- SHORT
M 0101010 0101010 0 0 0 000 0 0
TM_PERMIT_RESULT
Router#

```

# show fm ipv6 traffic-filter

To display the IPv6 information, use the **show fm ipv6 traffic-filter** command.

```
show fm ipv6 traffic-filter {all | {interface interface interface-number}}
```

Syntax Description	all	Displays IPv6 traffic filter information for all interfaces.
	<b>interface</b> <i>interface</i>	Displays IPv6 traffic filter information for the specified interface; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , <b>atm</b> , and <b>ge-wan</b> .
	<i>interface-number</i>	Module and port number; see the “Usage Guidelines” section for valid values.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

**Examples** This example shows how to display the IPv6 information for a specific interface:

```
Router# show fm ipv6 traffic-filter interface vlan 50
-----
FM_FEATURE_IPV6_ACG_INGRESS Name:testipv6 i/f: Vlan50
=====
DPort - Destination Port SPort - Source Port Pro - Protocol
X - XTAG TOS - TOS Value Res - VMR Result
RFM - R-Recirc1 Flag MRTNP - M-Multicast Flag R - Reflexive flag
- F-Fragment flag - T-Tcp Control N - Non-cachable
- M-More Fragments - P-Mask Priority(H-High, L-Low)
Adj1 - Adj1 Index T - M(Mask)/V(Value) FM - Flow Mask
NULL - Null FM SAO - Source Only FM DAO - Dest1 Only FM
SADA - Sour1& Dest1 Only VSADA - Vlan SADA Only FF - Full Flow
VFF - Vlan Full Flow F-VFF - Either FF or VFF A-VSD - Atleast VSADA
A-FF - Atleast FF A-VFF - Atleast VFF A-SON - Atleast SAO
A-DON - Atleast DAO A-SD - Atleast SADA SHORT - Shortest
A-SFF - Any short than FF A-EFF - Any except FF A-EVFF- Any except VFF
A-LVFF- Any less than VFF ERR - Flowmask Error
```

```
show fm ipv6 traffic-filter
```

```

+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
;Indx;T; Dest IPv6 Addr ; Source IPv6
Addr ;Pro;RFM;X;MRTNP;Adj1; FM ;
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
4 V 0:500E::
500D::4 0 -F- - ----L ---- Shorte
M 0:FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 0 4
TM_SOFT_BRIDGE_RESULT
5 V 0:500E::
500D::4 47 --- - ----L ---- Shorte
M 0:FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 555 0
TM_PERMIT_RESULT
3 V 500E::
500D::4 0 -F- - ----L ---- Shorte
M FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 0 4
TM_SOFT_BRIDGE_RESULT
4 V 500E::
500D::4 47 --- - ----L ---- Shorte
M FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 555 0
TM_PERMIT_RESULT
5 V
:: :: 0 -F- - ----L ---- Shorte
M
:: :: 0 4
TM_SOFT_BRIDGE_RESULT
6 V
:: :: 0 -F- - ----L ---- Shorte
M
:: :: 0 4
TM_SOFT_BRIDGE_RESULT
7 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 555 0
TM_PERMIT_RESULT
8 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 555 0
TM_PERMIT_RESULT
9 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 555 0
TM_PERMIT_RESULT
40 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 555 0
TM_PERMIT_RESULT
44 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 555 0
TM_PERMIT_RESULT
45 V
:: :: 58 --- - ----L ---- Shorte
M

```

```

:: :: 555 0
TM_PERMIT_RESULT
43 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 555 0
TM_PERMIT_RESULT
44 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 555 0
TM_PERMIT_RESULT
45 V
:: :: 0 --- - ----L ---- Shorte
M
:: :: 0 0
TM_L3_DEN\_RESULT
Router#

```

This example shows how to display the IPv6 information for all interfaces:

```
Router# show fm ipv6 traffic-filter all
```

```

-----
FM_FEATURE_IPV6_ACG_INGRESS Name:testipv6 i/f: Vlan50
=====
DPort - Destination Port SPort - Source Port Pro - Protocol
X - XTAG TOS - TOS Value Res - VMR Result
RFM - R-Recirc1 Flag MRTNP - M-Multicast Flag R - Reflexive flag
- F-Fragment flag - T-Tcp Control N - Non-cachable
- M-More Fragments - P-Mask Priority(H-High, L-Low)
Adj1 - Adj1 Index T - M(Mask)/V(Value) FM - Flow Mask
NULL - Null FM SAO - Source Only FM DAO - Dest1 Only FM
SADA - Sour1& Dest1 Only VSADA - Vlan SADA Only FF - Full Flow
VFF - Vlan Full Flow F-VFF - Either FF or VFF A-VSD - Atleast VSADA
A-FF - Atleast FF A-VFF - Atleast VFF A-SON - Atleast SAO
A-DON - Atleast DAO A-SD - Atleast SADA SHORT - Shortest
A-SFF - Any short than FF A-EFF - Any except FF A-EVFF- Any except VFF
A-LVFF- Any less than VFF ERR - Flowmask Error
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
---+---+---+---+---+---+---+---+---+---+
;Indx;T; Dest IPv6 Addr ; Source IPv6
Addr ;Pro;RFM;X;MRTNP;Adj1; FM ;
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
---+---+---+---+---+---+---+---+---+
4 V 0:500E::
500D::4 0 -F- - ----L ---- Shorte
M 0:FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 0 4
TM_SOFT_BRIDGE_RESULT
5 V 0:500E::
500D::4 47 --- - ----L ---- Shorte
M 0:FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 555 0
TM_PERMIT_RESULT
3 V 500E::
500D::4 0 -F- - ----L ---- Shorte
M FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 0 4
TM_SOFT_BRIDGE_RESULT
4 V 500E::
500D::4 47 --- - ----L ---- Shorte
M FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 555 0
TM_PERMIT_RESULT

```

```
show fm ipv6 traffic-filter
```

```

5 V
:: :: 0 -F- - ----L ---- Shorte
M
:: :: 0 4
TM_SOFT_BRIDGE_RESULT
6 V
:: :: 0 -F- - ----L ---- Shorte
M
:: :: 0 4
TM_SOFT_BRIDGE_RESULT
7 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 555 0
TM_PERMIT_RESULT
8 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 555 0
TM_PERMIT_RESULT
9 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 555 0
TM_PERMIT_RESULT
40 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 555 0
43 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 555 0
1
1 Output is truncated
1
Interface(s) using this IPv6 Ingress Traffic Filter:
V150,

```

# show fm nat netflow data

To display the information about the NAT-related NetFlow data, use the **show fm nat netflow data** command.

## show fm nat netflow data

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

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the information about the NAT-related NetFlow data:

```
Router> show fm nat netflow data
FM Pattern with stat push disabled: 4
Default/TCP/UDP Timeouts:
Def s/w timeout: 86400 h/w timeout: 300 Pattern(ingress): 4
Pattern(egress): 4 Push interval: 4333
TCP s/w timeout: 86400 h/w timeout: 300 Pattern(ingress): 4
Pattern(egress): 4 Push interval: 4333
UDP s/w timeout: 300 h/w timeout: 300 Pattern(ingress): 3
Pattern(egress): 3 Push interval: 400
Port Timeouts:
Idle timeout :3600 secs
Fin/Rst timeout :40 secs
Fin/Rst Inband packets sent per timeout :40000
Netflow mode to lero-out Layer4 information for fragment packet lookup :
Enabled
Router>
```

# show fm reflexive

To display the information about the reflexive entry for the dynamic feature manager, use the **show fm reflexive** command.

**show fm reflexive**

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

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the information about the reflexive entry for the dynamic feature manager:

```
Router# show fm reflexive
  Reflexive hash table:
    Vlan643:refacl, OUT-REF, 64060E0A, 64060D0A, 0, 0, 7, 783, 6

Router#
```

# show fm summary

To display a summary of feature manager information, use the **show fm summary** command.

## **show fm summary**

<b>Syntax Description</b>	This command has no keywords or arguments.
---------------------------	--

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Examples</b>	This example shows how to display a summary of feature manager information:
-----------------	---

```
Router# show fm summary
Current global ACL merge algorithm:BDD
Interface:FastEthernet5/40
  ACL merge algorithm used:
    inbound direction: ODM
    outbound direction:BDD
  TCAM screening for features is ACTIVE outbound
  TCAM screening for features is ACTIVE inbound
Interface:FastEthernet5/56
  ACL merge algorithm used:
    inbound direction: ODM
    outbound direction:BDD
  TCAM screening for features is ACTIVE outbound
  TCAM screening for features is INACTIVE inbound
1
1
1
Router#
```

## show fm vlan

To display the information about the per-VLAN feature manager, use the **show fm vlan** command.

**show fm vlan** *vlan-id*

<b>Syntax Description</b>	<i>vlan-id</i>	VLAN ID; valid values are from 1 to 4094.
<b>Defaults</b>	This command has no default settings.	
<b>Command Modes</b>	EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the information about the per-VLAN feature manager:

```
Router# show fm vlan 1
hw[EGRESS] = 4, hw[INGRESS] = 4
hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 0
mcast = 0
priority = 5
reflexive = 0
vacc_map : map4
inbound label: 5
merge_err: 0
protocol: ip
feature #: 4
feature id: FM_VACL
map_name: map4
seq #: 40
(only for IP_PROT) DestAddr SrcAddr Dpt Spt L4OP TOS Est prot Rslt
vmr IP value # 4: 0101010 0101010 0 0 0 0 0 6 permit
vmr IP mask # 4: 0101010 0101010 0 0 0 0 0 FF
vmr IP value # 5: 0101010 0101010 0 0 0 0 0 44 permit
vmr IP mask # 5: 0101010 0101010 0 0 0 0 0 FF
vmr IP value # 3: 0101010 0101010 0 0 0 0 0 0 deny
vmr IP mask # 3: 0101010 0101010 0 0 0 0 0 0
seq #: 65536
(only for IP_PROT) DestAddr SrcAddr Dpt Spt L4OP TOS Est prot Rslt
vmr IP value # 4: 0101010 0101010 0 0 0 0 0 0 permit
vmr IP mask # 4: 0101010 0101010 0 0 0 0 0 0
outbound label: 6
merge_err: 0
protocol: ip
feature #: 4
feature id: FM_VACL
map_name: map4
seq #: 40
(only for IP_PROT) DestAddr SrcAddr Dpt Spt L4OP TOS Est prot Rslt
vmr IP value # 4: 0101010 0101010 0 0 0 0 0 6 permit
```

```
vmr IP mask # 4: 0101010 0101010 0 0 0 0 0 FF
vmr IP value # 5: 0101010 0101010 0 0 0 0 0 44 permit
vmr IP mask # 5: 0101010 0101010 0 0 0 0 0 FF
vmr IP value # 3: 0101010 0101010 0 0 0 0 0 0 deny
vmr IP mask # 3: 0101010 0101010 0 0 0 0 0 0
seq #: 65536
(only for IP_PROT) DestAddr SrcAddr Dpt Spt L4OP TOS Est prot Rslt
vmr IP value # 4: 0101010 0101010 0 0 0 0 0 0 permit
vmr IP mask # 4: 0101010 0101010 0 0 0 0 0 0
```

# show icc

To display the information about the ICC counter and status, use the **show icc** command.

```
show icc {counters | status}
```

Syntax Description	counters	Specifies the counter information.
	status	Specifies the status information.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the information about the ICC counter:

```
Router# show icc counters
total tx RPC packets to slot 4 LCP = 0
  detail by request id: (<request-id>=<number-of-packets>)
    5 =0          7 =0          8 =0          40=0
    44=0         45=0         44=0         47=0
    48=0         49=0         50=0
total rx RPC packets from slot 4 LCP = 0
  detail by request id: (<request-id>=<number-of-packets>)
    5 =5          7 =7          8 =44         40=4
    44=4         45=5         44=4         47=67
    48=7         49=459        50=59
total tx MCAST-SP packets to slot 4 LCP = 0
  detail by request id: (<request-id>=<number-of-packets>)
    6 =0          7 =0          8 =0          9 =0
    45=0         44=0
total rx MCAST-SP packets from slot 4 LCP = 0
  detail by request id: (<request-id>=<number-of-packets>)
    6 =4          7 =4          8 =4          9 =4
    45=44        44=67
total tx L3-MGR packets to slot 4 LCP = 0
  detail by request id: (<request-id>=<number-of-packets>)
    4 =0          5 =0          3 =0
total rx L3-MGR packets from slot 4 LCP = 0
  detail by request id: (<request-id>=<number-of-packets>)
    4 =4          5 =5          3 =4
Router#
```

This example shows how to display the information about the ICC status:

```
Router# show icc status
Class Name           Msgs Pending  Max Pending  Total Sent
-----
   5 RPC              0             3            403
   3 MSC              0             4             4
   5 L3-MGR           0             4           4473
  43 TCAM-API         0            40            56
Router#
```

# show idprom

To display the IDPROMs for FRUs, use the **show idprom** command.

**show idprom** { **all** | *frutype* | **interface** *interface slot* } [**detail**]

Syntax Description		
<b>all</b>		Displays the information for all FRU types.
<i>frutype</i>		Type of FRU to display information; see the “Usage Guidelines” section for valid values.
<b>interface</b> <i>interface slot</i>		Specifies the interface to display information; valid values are as follows: <ul style="list-style-type: none"> <li>• <i>interface</i>—GigabitEthernet</li> <li>• <i>slot</i>—1 to 13</li> </ul> See the “Usage Guidelines” section for additional information.
<b>detail</b>		(Optional) Displays the details of the IDPROM data (verbose).

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Valid *frutypes* are as follows:

- **backplane**—No arguments.
- **clock number**—1 and 2.
- **earl slot**—See the following paragraph for valid values.
- **module slot**—See the following paragraph for valid values.
- **rp slot**—See the following paragraph for valid values.
- **power-supply**—1 and 2.
- **supervisor slot**—See the following paragraph for valid values.
- **vtt number**—1 to 3.

The *slot* argument designates the module and port number. Valid values for *slot* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

Use the **show idprom backplane** command to display the chassis serial number.

The optional **interface interface slot** keyword and arguments are supported on GBIC security-enabled interfaces only.

**Examples**

This example shows how to display IDPROM information for clock 1:

```
Router> show idprom clock 1
IDPROM for clock #4
(FRU is 'Clock FRU')
OEM String = 'Cisco Systems'
Product Number = 'WS-C6000-CL'
Serial Number = 'SMT03073445'
Manufacturing Assembly Number = '73-3047-04'
Manufacturing Assembly Revision = 'A0'
Hardware Revision = 410
Current supplied (+) or consumed (-) = 01000A
Router>
```

This example shows how to display IDPROM information for power supply 1:

```
Router> show idprom power-supply 1
IDPROM for power-supply #4
(FRU is '440/550v AC power supply, 4360 watt')
OEM String = 'Cisco Systems, Incl'
Product Number = 'WS-CAC-4300W'
Serial Number = 'ACP03050004'
Manufacturing Assembly Number = '34-0948-04'
Manufacturing Assembly Revision = 'A0'
Hardware Revision = 410
Current supplied (+) or consumed (-) = 571460A
Router>
```

This example shows how to display detailed IDPROM information for power supply 1:

```
Router# show idprom power-supply 1 detail
IDPROM for power-supply #4
IDPROM image:

(FRU is '440/550v AC power supply, 4360 watt')

IDPROM image block #0:
hexadecimal contents of block:
00: AB AB 04 90 44 BE 04 00 00 05 AB 04 00 04 43 69      1111111111111111Ci
40: 73 63 6F 50 53 79 73 74 65 6D 73 5C 50 49 6E 63      sco Systems, Inc
50: 5E 00 57 53 5D 43 44 43 5D 34 33 30 30 57 00 00      11WS-CAC-4300W11
30: 00 00 00 00 00 00 00 44 43 50 30 33 30 35 30 30 30      11111111ACP0305000
40: 34 00 00 00 00 00 00 00 00 00 33 34 5D 30 39 34      411111111134-094
50: 38 5D 30 34 00 00 00 00 00 00 44 30 00 00 00 00      8-04111111A01111
60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00      1111111111111111
70: 00 00 00 04 00 00 00 00 00 00 09 00 0C 00 03      1111111111111111
80: 00 04 00 06 00 04 00 00 00 00 0A BA 00 00 00 00      1111111111111111

block-signature = 0xABAB, block-version = 4,
block-length = 444, block-checksum = 4545

*** common-block ***
IDPROM capacity (bytes) = 556 IDPROM block-count = 5
FRU type = (0xAB04,4)
OEM String = 'Cisco Systems, Incl'
Product Number = 'WS-CAC-4300W'
Serial Number = 'ACP03050004'
Manufacturing Assembly Number = '34-0948-04'
Manufacturing Assembly Revision = 'A0'
Hardware Revision = 410
```

```

Manufacturing bits = 0x0 Engineering bits = 0x0
SNMP OID = 91451314161410
Power Consumption = 5746 centiamperes RMA failure code = 0-0-0-0
*** end of common block ***

IDPROM image block #4:
hexadecimal contents of block:
00: AB 04 04 44 05 5F 00 00 00 00 00 00 00 0A BA 11111_1111111111
40: 0A BA 00 46 1111

block-signature = 0xAB04, block-version = 4,
block-length = 50, block-checksum = 607

*** power supply block ***
feature-bits: 00000000 00000000
rated current at 440v: 5746 rated current at 550v: 5746 (centiamperes)
CISCO-STACK-MIB SNMP OID = 55 *** end of power supply block ***

```

```

End of IDPROM image
Router#

```

This example shows how to display IDPROM information for the backplane:

```

Router# show idprom backplane
IDPROM for backplane #0
(FRU is 'Catalyst 6000 9-slot backplane')
OEM String = 'Cisco Systems'
Product Number = 'WS-C6009'
Serial Number = 'SCA030900JA'
Manufacturing Assembly Number = '73-3046-04'
Manufacturing Assembly Revision = 'A0'
Hardware Revision = 410
Current supplied (+) or consumed (-) = 01000A
Router#

```

This example shows how to display IDPROM information from a GBIC security-enabled interface:

```

Router# show idprom interface g5/1
GBIC Serial EEPROM Contents:
Common block:
Identifier :
Connector :
Transceiver
Speed :
Media :
Technology :
Link Length :
GE Comp Codes :
SONET Comp Codes :
Encoding : 8B40B
BR, Nominal : 45x400 MHz
Length(9u) : GBIC does not support single mode fibre,
or the length information must be determined from
the transceiver technology1
Length(50u) : GBIC does not support 50 micron multi-mode fibre,
or the length information must be determined from
the transceiver technology1
Length(6515u) : GBIC does not support 6515 micron multi-mode fibre,
or the length information must be determined from
the transceiver technology1
Length(Copper) : GBIC does not support copper cables,
or the length information must be determined from
the transceiver technology1
Vendor Name : IBM

```

```
Vendor OUI : 0x8 0x0 0x5A
Vendor PN : IBM45P45SN\
Vendor rev : CS40
CC_BASE : 0xC6
Extended ID Fields
Options : Loss of Signal implemented TX_FAULT signal implemented
TX_D
ISABLE is implemented and disables the serial output
BR, max : 5%
BR, min : 5%
Vendor SN : 54P70450005D6
Date code : 05074004
CC_EXT : 0xCE
Vendor Specific ID Fields:
0x00: 00 00 00 70 5E DF C4 69 50 E6 54 F9 05 D4 83 A5
0x40: 4B 0E 8B 00 00 00 00 00 00 00 00 7D 3F D9 4E
Router#
```

# show interfaces

To display traffic that is seen by a specific interface, use the **show interfaces** command.

```
show interfaces [{interface interface-number} | {null interface-number} | {vlan vlan-id}]
```

Syntax Description	
<i>interface</i>	(Optional) Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , and <b>port-channel</b> , <b>atm</b> , and <b>ge-wan</b> .
<i>interface-number</i>	(Optional) Module and port number; see the “Usage Guidelines” section for valid values.
<b>null</b> <i>interface-number</i>	(Optional) Specifies the null interface; the valid value is <b>0</b> .
<b>vlan</b> <i>vlan-id</i>	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The valid values for port-channel are from 1 to 308. The port-channel values that are from 257 to 282 are internally allocated, and are supported on the CSM and the FWSM only.

Statistics are collected on a per-VLAN basis for Layer 2-switched packets and Layer 3-switched packets. Statistics are available for both unicast and multicast traffic. The Layer 3-switched packet counts are available for both ingress and egress directions. The per-VLAN statistics are updated every 5 seconds.

In some cases, you might see a difference in the duplex mode that is displayed between the **show interfaces** command and the **show running-config** commands. In this case, 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.

The output of the **show interfaces GigabitEthernet** command displays an extra 4 bytes for every packet that is sent or received. This display occurs on the LAN ports on the GE-WAN module and other Catalyst 6500 series switch Gigabit Ethernet LAN modules. The extra 4 bytes are the Ethernet frame CRC in the input and output byte statistics.

## Examples

This example shows how to display traffic for a specific interface:

```
Router# show interfaces GigabitEthernet3/3
GigabitEthernet3/3 is up, line protocol is up (connected)
  Hardware is C6k 4000Mb 80513, address is 000f15305149c0 (bia 000f15305149c0)
  MTU 4500 bytes, BW 4000000 Kbit, DL\ 40 usec,
    reliability 555/555, txload 4/555, rxload 4/555
  Encapsulation 80514Q Virtual LAN, Vlan ID 41, loopback not set
  Keepalive set (40 sec)
  Full-duplex, 4000Mb/s, media type is LH
  input flow-control is off, output flow-control is on
  Clock mode is auto
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:49, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
L5 Switched: ucast: 360 pkt, 53040 bytes - mcast: 0 pkt, 0 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
  437 packets input, 48503 bytes, 0 no buffer
  Received 76 broadcasts (0 IP multicast)
  0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 0 multicast, 0 pause input
  0 input packets with dribble condition detected
  86 packets output, 55940 bytes, 0 underruns <=====
  0 output errors, 0 collisions, 0 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier, 0 PAUSE output
  0 output buffer failures, 0 output buffers swapped out
Router#
```

This example shows how to display traffic for a FlexWAN module:

```
Router# show interfaces pos 6/1/0.1
POS6/4/014 is up, line protocol is up
  Hardware is Packet over Sonet
  Internet address is 4141515/54
  MTU 4470 bytes, BW 455000 Kbit, DL\ 400 usec,
    reliability 555/555, txload 4/555, rxload 4/555
  Encapsulation FRAME-RELA\ <<<+++ no packets info after this line
Arches#sh mod 6
```

## show interfaces

```

Mod Ports Card Type                               Model                               Serial No1
-----
 6    0 5 port adapter FlexWAN                    WS-X6485-5PA                       SAD04340J\3

Mod MAC addresses                               Hw   Fw           Sw           Status
-----
 6  0004164451a534 to 0004164451a573  413  4515(5004055 4515(5004055 Ok

Mod Online Diag Status
-----
 6 Pass
Router#

```

# show interfaces accounting

To display the number of packets of each protocol type that have been sent through all configured interfaces, use the **show interfaces accounting** command.

```
show interfaces [{interface interface-number} | {null interface-number} | {vlan vlan-id}]
accounting
```

Syntax Description		
	<i>interface</i>	(Optional) Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , and <b>port-channel</b> , <b>atm</b> , and <b>ge-wan</b> .
	<i>interface-number</i>	(Optional) Module and port number; see the “Usage Guidelines” section for valid values.
	<b>null</b> <i>interface-number</i>	(Optional) Specifies the null interface; the valid value is <b>0</b> .
	<b>vlan</b> <i>vlan-id</i>	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines



### Note

The Pkts Out and Chars Out fields display IPv6 packet counts only. The Pkts In and Chars In fields display both IPv4 and IPv6 packet counts, except for tunnel interfaces. For tunnel interfaces, the IPv6 input packets are counted as IPv6 packets only.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The port channels from 257 to 282 are internally allocated and are supported on the CSM and the FWSM only.

If you do not enter any keywords, all counters for all modules are displayed.

**Examples** This example shows how to display the number of packets of each protocol type that have been sent through all configured interfaces:

```

Router# show interfaces gigabitethernet5/2 accounting
GigabitEthernet5/5
Protocol Pkts In Chars In Pkts Out Chars Out
IP       50554   50554000 0       0
DEC MOP  0       0         4       459
CDP      0       0         4       595
IPv6     44      834      96      434658
Router#

```

Table 2-37 describes the fields that are shown in the example.

**Table 2-37** *show interfaces accounting Command Output Fields*

Field	Description
Protocol	Protocol that is operating on the interface.
Pkts In	Number of IPv4 packets received for the specified protocol.
Chars In	Number of IPv4 characters received for the specified protocol.
Pkts Out	Number of hardware-switched IPv6 packets transmitted for the specified protocol.
Chars Out	Number of IPv6 characters transmitted for the specified protocol.

# show interfaces capabilities

To display the interface capabilities for a module, an interface, or all interfaces, use the **show interfaces capabilities** command.

**show interfaces** [*interface interface-number*] **capabilities** [{**module number**}]

Syntax Description		
<i>interface</i>	(Optional) Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , <b>atm</b> , and <b>port-channel</b> , and <b>ge-wan</b> .	
<i>interface-number</i>	Module and port number; see the “Usage Guidelines” section for valid values.	
<b>module number</b>	(Optional) Specifies the module number; see the “Usage Guidelines” section for valid values.	

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 2 to 13 and valid values for the port number are from 1 to 48.

The **port-channel** values are from 0 to 282; values from 257 to 282 are supported on the CSM and the FWSM only.

**Examples**

This example shows how to display the interface capabilities for a module:

```
Router# show interfaces capabilities module 6
FastEthernet6/4
Dot4x: yes
Model: WS-X6548-RJ-45
Type: 40/400BaseTX
Speed: 40,400,auto
Duplex: half,full
Trunk encaps type: 80514Q,ISL
Trunk mode: on,off,desirable,nonegotiate
Channel: yes
Broadcast suppression: percentage(0-400)
Flowcontrol: rx-(off,on),tx-(none)
Membership: static
Fast Start: yes
QOS scheduling: rx-(4q4t), tx-(5q5t)
CoS rewrite: yes
ToS rewrite: yes
Inline power: no
SPAN: source/destination
UDLD yes
Link Debounce: yes
Link Debounce Time: no
Ports on ASIC: 4-45
Port-Security: yes
Router#
```

This example shows how to display the interface capabilities for an interface:

```
Router# show interfaces fastethernet 4/1 capabilities
FastEthernet4/4
Model: WS-X6348-RJ-45
Type: 40/400BaseTX
Speed: 40,400,auto
Duplex: half,full
Trunk encaps type: 80514Q,ISL
Trunk mode: on,off,desirable,nonegotiate
Channel: yes
Broadcast suppression: percentage(0-400)
Flowcontrol: rx-(off,on),tx-(none)
Fast Start: yes
QOS scheduling: rx-(4q4t), tx-(5q5t)
CoS rewrite: yes
ToS rewrite: yes
Inline power: no
SPAN: source/destination
```

This example shows how to display the port-channel interface capabilities:

```
Router# show interfaces port-channel 12 capabilities
Port-channel45
Model: NO IDPROM
Type: unknown
Speed: 40,400,4000,auto
Duplex: half,full
Trunk encaps type: 80514Q,ISL
Trunk mode: on,off,desirable,nonegotiate
Channel: yes
```

```
Broadcast suppression: percentage (0-400)
Flowcontrol:          rx- (off,on) ,tx- (none)
Fast Start:          yes
QOS scheduling:      rx- (4q4t) , tx- (4q4t)
CoS rewrite:         yes
ToS rewrite:         yes
Inline power:        no
SPAN:                source/destination
Router#
```

# show interfaces counters

To display the traffic that the physical interface sees, use the **show interfaces counters** command.

```
show interfaces [interface] counters [errors | etherchannel | {module number} | {protocol status} | {trunk [module number]}]
```

Syntax Description	
<i>interface</i>	(Optional) Interface type; for a list of valid values, see the “Usage Guidelines” section.
<b>errors</b>	(Optional) Displays the interface-error counters.
<b>etherchannel</b>	(Optional) Displays information about the EtherChannel interface.
<b>module number</b>	(Optional) Displays the module number; see the “Usage Guidelines” section for valid values.
<b>protocol status</b>	(Optional) Displays the current status of the enabled protocols.
<b>trunk</b>	(Optional) Displays the interface-trunk counters.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **show interfaces** [*interface*] **counters** command displays the number of all of the packets arriving and includes the number of packets that may be dropped by the interface due to the storm-control settings. To display the total number of dropped packets, you can enter the **show interfaces** [*interface*] **counters storm-control** command.

If you do not enter any keywords, all counters for all modules are displayed.

When you enter the *interface*, these formats can be used:

- *card-type* {*slot*}/{*first-port*} - {*last-port*}
- *card-type* {*slot*}/{*first-port*} - {*last-port*}

You can define a single port range per command entry. If you specify a range of ports, the range must consist of the same slot and port type.

When you define a range, you must enter a white space between the first port and the hyphen (-) as follows:

```
show interfaces gigabitethernet7/4 -7 counters
```

The **module number** keyword and argument designate the module number and limit the display to interfaces on the module. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values for the module number are from 1 to 13.

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

- **ethernet**
- **fastethernet**
- **gigabitethernet**
- **tengigabitethernet**
- **port-channel interface-number**—Valid values are from 1 to 282; values from 257 to 282 are supported on the CSM and the FWSM only.

When you enter the **show interfaces interface counters etherchannel** command, follow these guidelines:

- If *interface* specifies a physical port, the command displays this message, “Etherchnl not enabled on this interface.”
- If *interface* is omitted, the command displays the counters for all port channels (in the system) and for their associated physical ports.
- If *interface* specifies a port channel, the command displays the counters for the port channel and all of the physical ports that are associated with it. In addition, when you enter the command specifying the primary aggregator in a LACP port channel with multiple aggregators, the output includes the statistics for all of the aggregators in the port channels and for the ports that are associated with them.

## Examples

This example shows how to display the error counters for a specific module:

```
Router# show interfaces counters errors module 1
Port          Align-Err    FCS-Err    Xmit-Err    Rcv-Err    UnderSize
Gi4/4          0            0          0           0          0
Gi4/5          0            0          0           0          0

Port          Single-Col  Multi-Col   Late-Col   Excess-Col  Carri-Sen    Runts    Giant
s
Gi4/4          0          0          0          0           0           0        0
Gi4/5          0          0          0          0           0           0        0
Router#
```

This example shows how to display traffic that is seen by a specific module:

```
Router# show interfaces counters module 1

Port          InOctets    InUcastPkts  InMcastPkts  InBcastPkts
Gi4/4          0           0            0            0
Gi4/5          0           0            0            0

Port          OutOctets    OutUcastPkts  OutMcastPkts  OutBcastPkts
Gi4/4          0           0            0            0
Gi4/5          0           0            0            0
Router#
```

This example shows how to display the trunk counters for a specific module:

```
Router# show interfaces counters trunk module 1

Port          TrunkFramesTx  TrunkFramesRx  WrongEncap
Gi4/4          0              0              0
Gi4/5          0              0              0
Router#
```

## ■ show interfaces counters

This example shows how to display the counters for all port channels (in the system) and their associated physical ports:

```
Router# show interfaces counters etherchannel
Port          InOctets    InUcastPkts  InMcastPkts  InBcastPkts
Po4           5548        4             59            4
Fa3/48        5548        4             59            4
Po5           44897       5             54            5
Fa3/45        5878        4             57            4
Fa3/46        6049        4             57            4
Po3           0           0             0             0
Po5           6073        4             57            4
Fa3/44        6073        4             57            4
Po5A          7844        4             53            4
Fa3/43        7844        4             53            4

Port          OutOctets    OutUcastPkts  OutMcastPkts  OutBcastPkts
Po4           4333        4             54            4
Fa3/48        4333        4             54            4
Po5           9535        5             46            5
Fa3/45        4766        4             53            4
Fa3/46        4766        4             53            4
Po3           0           0             0             0
Po5           47554       4             544           4
Fa3/44        47554       4             544           4
Po5A          474456     4             5669          4
Fa3/43        474456     4             5669          4
```

This example shows how to display the counters for a specific port channel and the counters for the associated physical ports:

```
Router# show interfaces port-channel2 counters etherchannel

Port          InOctets    InUcastPkts  InMcastPkts  InBcastPkts
Po5           6007        4             34            4
Fa3/48        6007        4             34            4

Port          OutOctets    OutUcastPkts  OutMcastPkts  OutBcastPkts
Po5           4458        4             55            4
Fa3/48        4458        4             55            4
Router#
```

This example shows how to display the discard count and the level settings for each mode:

```
Router# show interfaces counters storm-control

Port          UcastSupp %    McastSupp %    BcastSupp %    TotalSuppDiscards
Fa5/4         40010          40010          40010          0
Fa5/5         40010          40010          40010          0
Fa5/3         40010          40010          40010          0
1
1
1
Router#
```

## Related Commands

Command	Description
<a href="#">clear counters</a>	Clears the interface counters.

# show interfaces debounce

To display the status and configuration for the debounce timer, use the **show interfaces debounce** command.

```
show interfaces [{interface interface-number} | {null interface-number} | {vlan vlan-id}]
debounce [module num]
```

Syntax Description		
<i>interface</i>	(Optional) Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>port-channel</b> , <b>pos</b> , <b>atm</b> , and <b>ge-wan</b> .	
<i>interface-number</i>	(Optional) Module and port number; see the “Usage Guidelines” section for valid values.	
<b>null</b> <i>interface-number</i>	(Optional) Specifies the null interface; the valid value is <b>0</b> .	
<b>vlan</b> <i>vlan-id</i>	(Optional) Specifies the VLAN; valid values are from 1 to 4094.	
<b>module</b> <i>num</i>	(Optional) Limits the display to interfaces on the specified module.	

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The debounce timer is not supported on the 10-Gigabit Ethernet module (WSX-6502-10GE). The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48. The port-channel values are from 0 to 282; values from 257 to 282 are supported on the CSM and the FWSM only.

---

**Examples**

This example shows how to display the debounce configuration of an interface:

```
Router# show interfaces GigabitEthernet1/1 debounce
Port    Debounce time  Value
Gi4/4   enable         400
Router#
```

---

**Related Commands**

Command	Description
<a href="#">link debounce</a>	Enables the debounce timer on an interface.

# show interfaces description

To display a description and a status of an interface, use the **show interfaces description** command.

**show interfaces** [*interface*] **description**

<b>Syntax Description</b>	<i>interface</i> (Optional) Interface type; for a list of valid values, see the “Usage Guidelines” section.
---------------------------	---

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

**Command Modes** EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** When you enter the *interface* value, these formats can be used:

- *card-type* {*slot*}/{*first-port*} - {*last-port*}
- *card-type* {*slot*}/{*first-port*} - {*last-port*}

You can define a single port range per command entry. If you specify a range of ports, the range must consist of the same slot and port type. When you define a range, you must enter a space before and after the hyphen (-) as follows:

```
show interfaces gigabitethernet7/4 - 7 counters broadcast
```

Possible valid values for *card-type* are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **port-channel**, **pos**, **atm**, and **ge-wan**.

The port-channel values are from 0 to 282; values from 257 to 282 are supported on the CSM and the FWSM only.

**Examples** This example shows how to display the information for all interfaces:

```
Router# show interfaces description
Interface Status      Protocol Description
PO0/0     admin down    down    First POS interface
PO0/4     admin down    down
Gi4/0     up            up      GigE to server farm
Router#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>description</b>	Includes a specific description about the DSP interface.

# show interfaces flowcontrol

To display flow-control information, use the **show interfaces flowcontrol** command.

```
show interfaces [interface [mod]] flowcontrol [module number]
```

Syntax Description	
<i>interface</i>	(Optional) Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>port-channel</b> , <b>pos</b> , <b>atm</b> , and <b>ge-wan</b> .
<i>mod</i>	(Optional) Module and port number.
<b>module number</b>	(Optional) Specifies the module number; see the “Usage Guidelines” section for valid values.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The *mod* argument designates the module and port number. Valid values for *mod* depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 1 to 13 and valid values for the port number are from 1 to 48.

The **module number** keyword and argument designate the module number and limit the display to interfaces on the module. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values for the module number are from 1 to 13.

The port-channel values are from 0 to 282; values from 257 to 282 are supported on the CSM and the FWSM only.

**Examples**

This example shows how to display flow-control information for all interfaces:

```
Router# show interfaces flowcontrol

Port  Send      FlowControl  Receive FlowControl  RxPause TxPause
      admin    oper        admin    oper
-----
Gi4/4  desired  off         off      off         0       0
Gi4/5  desired  off         off      off         0       0
Gi3/4  on       on          on       on          0       0
1
1
1
Gi8/5  desired  off         off      off         0       0
Gi8/3  desired  off         off      off         0       0
Gi8/4  desired  off         off      off         0       0
Router#
```

This example shows how to display flow-control information for a specific interface:

```
Router# show interfaces gigabitethernet 8/2 flowcontrol

Port  Send      FlowControl  Receive FlowControl  RxPause TxPause
      admin    oper        admin    oper
-----
Gi8/5  desired  off         off      off         0       0
Router#
```

Table 2-38 describes the fields that are shown in the example.

**Table 2-38** show port flowcontrol Command Output Fields

Field	Description
Port	Interface type and module and port number.
Send admin	Flow-control operation for admin state. On indicates that the local port is allowed to send pause frames to remote ports, off indicates that the local port is prevented from sending pause frames to remote ports, and desired indicates predictable results whether a remote port is set to <b>receive on</b> , <b>receive off</b> , or <b>receive desired</b> .
Send oper	Current flow-control operation. On indicates that the local port is allowed to send pause frames to remote ports, off indicates that the local port is prevented from sending pause frames to remote ports, and desired indicates predictable results whether a remote port is set to <b>receive on</b> , <b>receive off</b> , or <b>receive desired</b> .
Receive admin	Flow-control operation for admin state. On indicates that the local port is allowed to send pause frames to remote ports, off indicates that the local port is prevented from sending pause frames to remote ports, and desired indicates predictable results whether a remote port is set to <b>send on</b> , <b>send off</b> , or <b>send desired</b> .

*Table 2-38 show port flowcontrol Command Output Fields (continued)*

Field	Description
Receive oper	Current flow-control operation. On indicates that the local port is allowed to send pause frames to remote ports, off indicates that the local port is prevented from sending pause frames to remote ports, and desired indicates predictable results whether a remote port is set to <b>send on</b> , <b>send off</b> , or <b>send desired</b> .
RxPause	Number of pause frames that are received.
TxPause	Number of pause frames that are transmitted.

**Related Commands**

Command	Description
<a href="#">flowcontrol</a>	Configures a port to send or receive pause frames.

# show interfaces private-vlan mapping

To display the information about the PVLAN mapping for VLAN SVIs, use the **show interfaces private-vlan mapping** command.

**show interfaces** [*interface interface-number*] **private-vlan mapping** [**active**]

Syntax Description		
<i>interface</i>	(Optional) Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , <b>atm</b> , and <b>ge-wan</b> .	
<i>interface-number</i>	Module and port number; see the “Usage Guidelines” section for valid values.	
<b>active</b>	(Optional) Displays the active interfaces only.	

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command displays SVI information only.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 1 to 13 and valid values for the port number are from 1 to 48.

**Examples** This example shows how to display the information about the PVLAN mapping:

```
Router# show interfaces private-vlan mapping
Interface Secondary VLAN Type
-----
vlan5      304      community
vlan5      305      community
Router#
```

Related Commands	Command	Description
	<a href="#">private-vlan</a>	Configures PVLANS and the association between a PVLAN and a secondary VLAN.
	<a href="#">private-vlan mapping</a>	Creates a mapping between the primary and the secondary VLANs so that both VLANs share the same primary VLAN SVI.

## show interfaces status

To display the interface status or a list of interfaces in an error-disabled state on LAN ports only, use the **show interfaces status** command.

```
show interfaces [interface interface-number] status [err-disabled | module number]
```

Syntax Description	
<i>interface</i>	(Optional) Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , <b>atm</b> , and <b>ge-wan</b> .
<i>interface-number</i>	Module and port number; see the “Usage Guidelines” section for valid values.
<b>err-disabled</b>	(Optional) Displays the LAN ports in an error-disabled state.
<b>module number</b>	(Optional) Specifies the module number; see the “Usage Guidelines” section for valid values.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 1 to 13 and valid values for the port number are from 1 to 48.

This command is supported on LAN ports only.

The **module number** keyword and argument designate the module number and limit the display to the interfaces on the module. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values for the module number are from 1 to 13.

To find out if an interface is inactive, enter the **show interfaces status** command. If the interface is inactive, the Status field displays “inactive.” If the port is not inactive, the Status field displays “none.”

To find the packet and byte count, you can enter the **show interfaces counters** command or the **show interfaces interface interface-number status** command. The **show interfaces counters** command is the preferred command to use. In some cases, the packet and byte count of the **show interfaces interface interface-number status** command is incorrect.

**Examples**

This example shows how to display the status of all LAN ports:

```
Router# show interfaces status
```

```
Port      Name              Status      Vlan      Duplex Speed Type
Gi4/4          disabled    routed          full  4000 missing
Gi4/5          notconnect  4              full  4000 unknown (4)
Fa5/4          disabled    routed          auto  auto 40/400BaseTX
1
1
1
Port      Name              Status      Vlan      Duplex Speed Type
Fa5/48      disabled      4              auto  auto 40/400BaseTX
Fa5/49      disabled      4              auto  auto 40/400BaseTX
Gi7/4        disabled      4              full  4000 WDM-RXONL\
Gi7/5        disabled      4              full  4000 No Transceiver
Router#
```

This example shows how to display the packet and byte count of a specific LAN port:

```
Router# show interfaces fastethernet5/2 status
```

```
FastEthernet5/5
Switching path  Pkts In  Chars In  Pkts Out  Chars Out
      Processor      47      4550      50      5050
      Route cache    0         0         0         0
      Distributed cache 47      4550 506745847 5444846570
      Total          34      5440 506745837 5444848590
```

```
Router#
```

This example shows how to display the status of LAN ports in an error-disabled state:

```
Router# 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
Router#
```

**Related Commands**

Command	Description
<a href="#">errdisable detect cause</a>	Enables the error-disable detection.
<a href="#">show errdisable recovery</a>	Displays the information about the error-disable recovery timer.

# show interfaces summary

To display a summary of statistics for all interfaces that are configured on a networking device, use the **show interfaces summary** command.

**show interfaces** [*interface interface-number*] **summary** [**vlan**]

Syntax Description	
<i>interface</i>	(Optional) Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , <b>atm</b> , and <b>ge-wan</b> .
<i>interface-number</i>	Module and port number; see the “Usage Guidelines” section for valid values.
<b>vlan</b>	(Optional) Displays the total number of VLAN interfaces.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Separate counters for subinterfaces are not maintained and are not displayed in the **show interfaces summary** output.

**Examples** This example shows how to display a summary of statistics for all interfaces that are configured on a networking device:

```
Router# show interfaces summary
*: interface is up
IHQ: pkts in input hold queue IQD: pkts dropped from input queue
OHQ: pkts in output hold queue OQD: pkts dropped from output queue
RXBS: rx rate (bits/sec) RXPS: rx rate (pkts/sec)
TXBS: tx rate (bits/sec) TXPS: tx rate (pkts/sec)
TRTL: throttle count
Interface IHQ IQD OHQ OQD RXBS RXPS TXBS TXPS TRTL
-----
* FastEthernet0/0 0 0 0 0 0 0 0 0 0
Serial0/0 0 0 0 0 0 0 0 0 0
FastEthernet0/4 0 0 0 0 0 0 0 0 0
Serial0/4 0 0 0 0 0 0 0 0 0
Router#
```

This example shows how to display the total number of VLAN interfaces:

```
Router# show interfaces summary vlan
Total number of Vlan interfaces: 7
Vlan interfaces configured:
4,5,50,5000,3000-3004,4000
Router#
```



# show interfaces switchport

To display the administrative and operational status of a switching (nonrouting) port, use the **show interfaces switchport** command.

```
show interfaces [interface interface-number] switchport [brief] [module number]
```

Syntax Description	
<i>interface</i>	(Optional) Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , <b>atm</b> , and <b>ge-wan</b> .
<i>interface-number</i>	Module and port number; see the “Usage Guidelines” section for valid values.
<b>brief</b>	(Optional) Displays a brief summary of information.
<b>module number</b>	(Optional) Limits the display to interfaces on a specified module; see the “Usage Guidelines” section for valid values.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The *interface-number* designates the module and port number. Valid values depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 1 to 13 and valid values for the port number are from 1 to 48.

**Examples** This example shows how to display switch-port information using the **include** output modifier:

```
Router# show interfaces switchport | include VLAN
Name: Fa5/6
Access Mode VLAN: 500 (VLAN0500)
Trunking Native Mode VLAN: 4 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: ALL
1
1
1

Router#
```

This example shows how to display the configurations of two multiple VLAN access ports:

```
Router# show interfaces switchport
Name: Fa5/4
```

```

Switchport: Enabled
Administrative Mode: access
Operational Mode: access
Dot4q Ethertype: 0x8500
Operational Trunking Encapsulation: dot4q
Negotiation of Trunking: off
Access Mode VLAN: 400
Voice VLAN: 405
Trunking Native Mode VLAN: 4 (default)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: 900 ((Inactive)) 904 ((Inactive))
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 5-4004
Capture Mode Disabled
Capture VLANs Allowed: ALL

Name: Fa5/5
Switchport: Enabled
Administrative Mode: access
Operational Mode: down
Dot4q Ethertype: 0x8500
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 400
Voice VLAN: 403 ((inactive))
Trunking Native Mode VLAN: 4 (default)
1
1
1

```

This example shows how to display a brief summary of information:

```

Router# show interfaces switchport brief module 3
Port Status Op1Mode Op1Encap Channel-id Vlan
Fa3/4 connected access native -- 4
Fa3/7 disabled -- dot4q Po56 4
Fa3/43 connected access native -- 666
Router#

```

# show interfaces switchport backup

To display Flexlink pairs, use the **show interfaces switchport backup** command.

**show interfaces** [*interface interface-number*] **switchport backup**

Syntax Description	<i>interface</i>	(Optional) Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , <b>atm</b> , and <b>ge-wan</b> .
	<i>interface-number</i>	Module and port number; see the “Usage Guidelines” section for valid values.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The *interface-number* designates the module and port number. Valid values depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 1 to 13 and valid values for the port number are from 1 to 48.

**Examples** This example shows how to display all Flexlink pairs:

```
Router# show interfaces switchport backup
Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
-----
FastEthernet3/4      FastEthernet4/4      Active Up/Backup Standby
FastEthernet5/4      FastEthernet5/5      Active Down/Backup Up
FastEthernet3/5      FastEthernet5/4      Active Standby/Backup Up
Po4                  Po5                  Active Down/Backup Down
Router#
```

This example shows how to display a specific Flexlink port:

```
Router# show interfaces fastethernet 4/1 switchport backup
Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
-----
FastEthernet3/4      FastEthernet4/4      Active Up/Backup Standby
Router#
```

---

**Related Commands**

Command	Description
<a href="#">switchport backup</a>	Configures an interface as a Flexlink backup interface.

---

# show interfaces transceiver

To display information about the optical transceivers that have DOM enabled, use the **show interfaces transceiver** command.

```
show interfaces [interface interface-number] transceiver [threshold violations] [detail |
  {module number}]
```

Syntax Description		
<i>interface</i>	(Optional) Interface type; possible valid values are <b>gigabitethernet</b> and <b>tengigabitethernet</b> .	
<i>interface-number</i>	Module and port number; see the “Usage Guidelines” section for valid values.	
<b>threshold violations</b>	(Optional) Displays information about the interface transceiver threshold violations.	
<b>detail</b>	(Optional) Displays detailed information about the interface transceiver.	
<b>module number</b>	(Optional) Specifies the module number; see the “Usage Guidelines” section for valid values.	

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** After a transceiver is inserted, the software waits approximately 10 seconds before reading the diagnostic monitoring information. If you enter the **show interfaces transceiver** command before the software has read the diagnostic monitoring information, the following message is displayed:

```
Waiting for diagnostic monitoring information to settle down1
Please try again after a few seconds1
```

Wait a few seconds and reenter the **show interfaces transceiver** command.

The *interface interface-number* arguments are supported on interfaces that have a transceiver that has diagnostic monitoring enabled and the transceiver is in a module that supports the reading of diagnostic monitoring information.

**Examples** This example shows how to display transceiver information:

```
Router# show interfaces transceiver
If device is externally calibrated, only calibrated values are printed1
++ : high alarm, + : high warning, - : low warning, -- : low alarm1
NA or N/A: not applicable, Tx: transmit, Rx: receive1
mA: milliamperes, dBm: decibels (milliwatts)1
```

```

          Temperature  Voltage  Current      Optical  Optical
Port      (Celsius)    (Volts)  (mA)        Tx Power  Rx Power
-----
Gi4/4      4016           5109     014        -5515     N/A
Gi5/4      3515           5105     014        -5915     N/A
Gi5/5      4915           3130     010         714      -4817
Router#

```

This example shows how to display detailed transceiver information:

```

Router# show interfaces transceiver detail
mA: milliamperes, dBm: decibels (milliwatts), NA or N/A: not applicable
++ : high alarm, + : high warning, - : low warning, -- : low alarm
ASD readouts (if they differ), are reported in parentheses
The threshold values are calibrated

```

```

          High Alarm  High Warn  Low Warn  Low Alarm
          Threshold  Threshold  Threshold  Threshold
Port      (Celsius)  (Celsius)  (Celsius)  (Celsius)
-----
Gi4/4      4814           40010     40010     010       010
Gi4/5      3419           40010     40010     010       010
Gi5/4      4315           7010      6010      510       010
Gi5/5      3914           7010      6010      510       010

```

```

          High Alarm  High Warn  Low Warn  Low Alarm
          Threshold  Threshold  Threshold  Threshold
Port      (Volts)    (Volts)    (Volts)    (Volts)
-----
Gi4/4      3130           6150      6150      N/A       N/A
Gi4/5      3130           6150      6150      N/A       N/A
Gi5/4      5103           5150      5155      4175      4150
Gi5/5      5105           5150      5155      4175      4150

```

```

          High Alarm  High Warn  Low Warn  Low Alarm
          Threshold  Threshold  Threshold  Threshold
Port      (mA)        (mA)        (mA)        (mA)
-----
Gi4/4      010           43010     43010     N/A       N/A
Gi4/5      417           43010     43010     N/A       N/A
Gi5/4      5016          +         6010      4010      4010      510
Gi5/5      5518           6010      4010      4010      4010      510

```

```

          High Alarm  High Warn  Low Warn  Low Alarm
          Threshold  Threshold  Threshold  Threshold
Port      (dBm)        (dBm)        (dBm)        (dBm)
-----
Gi4/4      814           ++         814        814        N/A       N/A
Gi4/5      -918          814        814        N/A       N/A
Gi5/4      -4617         --         314        315        -013     -015
Gi5/5      018           314        315        -013     -015

```

```

          High Alarm  High Warn  Low Warn  Low Alarm
          Threshold  Threshold  Threshold  Threshold
Port      (dBm)        (dBm)        (dBm)        (dBm)
-----
Gi4/4      N/A           814        814        N/A       N/A
Gi4/5      -3019         814        814        N/A       N/A
Gi5/4      N/A           519        -617       -5815     -5815
Gi5/5      N/A           519        -617       -5815     -5815
Router#

```

This example shows how to display the threshold violations for all the transceivers on a Catalyst 6500 series switch:

```
Router# show interfaces transceiver threshold violations
Rx: Receive, Tx: Transmit1
DDDD: days, HH: hours, MM: minutes, SS: seconds

      Time since Last Known
      Time in slot   Threshold Violation   Type(s) of Last Known
Port   (DDDD:HH:MM:SS) (DDDD:HH:MM:SS)     Threshold Violation(s)
-----
Gi4/4   0000:00:03:44     Not applicable       Not applicable
Gi5/4   0000:00:03:40     0000:00:00:30       Tx bias high warning
                                           5015 mA > 4010 mA
                                           0000:00:00:30       Tx power low alarm
                                           -4710 dBm < -015 dBm
Gi5/5   0000:00:03:40     Not applicable       Not applicable

Router#
```

This example shows how to display the threshold violations for all transceivers on a specific module:

```
Router# show interfaces transceiver threshold violations module 2
lo: low, hi: high, warn: warning
DDDD: days, HH: hours, MM: minutes, SS: seconds

      Time since Last Known
      Time in slot   Threshold Violation   Type(s) of Last Known
Port   (DDDD:HH:MM:SS) (DDDD:HH:MM:SS)     Threshold Violation
-----
Gi5/4   0000:00:03:40     0000:00:00:30       Tx bias high warning
                                           5015 mA > 4010 mA
                                           0000:00:00:30       Tx power low alarm
                                           -4710 dBm < -015 dBm
Gi5/5   0000:00:03:40     Not applicable       Not applicable

Router#
```

This example shows how to display violations for the transceiver on a specific interface:

```
Router# show interfaces Gi2/1 transceiver threshold violations
Rx: Receive, Tx: Transmit1
DDDD: days, HH: hours, MM: minutes, SS: seconds

      Time since Last Known
      Time in slot   Threshold Violation   Type(s) of Last Known
Port   (DDDD:HH:MM:SS) (DDDD:HH:MM:SS)     Threshold Violation(s)
-----
Gi5/4   0000:00:03:40     0000:00:00:30       Tx bias high warning
                                           5015 mA > 4010 mA
                                           0000:00:00:30       Tx power low alarm
                                           -4710 dBm < -015 dBm

Router#
```

# show interfaces trunk

To display the interface-trunk information, use the **show interfaces trunk** command.

**show interfaces** [*interface interface-number*] **trunk** [**module number**]

Syntax Description		
<i>interface</i>	(Optional) Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , <b>atm</b> , and <b>ge-wan</b> .	
<i>interface-number</i>	(Optional) Module and port number; see the “Usage Guidelines” section for valid values.	
<b>module number</b>	(Optional) Specifies the module number; see the “Usage Guidelines” section for valid values.	

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** If you do not specify a keyword, only information for trunking ports is displayed.

The *interface-number* designates the module and port number. Valid values depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 1 to 13 and valid values for the port number are from 1 to 48.

The **module number** keyword and argument designate the module number and limit the display to interfaces on the module. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values for the module number are from 1 to 13.

**Examples** This example shows how to display the interface-trunk information for module 5:

```
Router# show interfaces trunk module 5
```

Port	Mode	Encapsulation	Status	Native vlan
Fa5/4	routed	negotiate	routed	4
Fa5/5	routed	negotiate	routed	4
Fa5/3	routed	negotiate	routed	4
Fa5/4	routed	negotiate	routed	4
Fa5/5	routed	negotiate	routed	4
Fa5/6	off	negotiate	not-trunking	40
Fa5/7	off	negotiate	not-trunking	40
Fa5/8	off	negotiate	not-trunking	4
Fa5/9	desirable	n-isl	trunking	4

## show interfaces trunk

```

Fa5/40 desirable negotiate not-trunking 4
Fa5/44 routed negotiate routed 4
Fa5/45 routed negotiate routed 4

```

```

1
1
1
Fa5/48 routed negotiate routed 4

```

## Port Vlans allowed on trunk

```

Fa5/4 none
Fa5/5 none
Fa5/3 none
Fa5/4 none
Fa5/5 none
Fa5/6 none
Fa5/7 none
Fa5/8 500
Fa5/9 4-4005
Fa5/40 none
Fa5/44 none
Fa5/45 none

```

```

1
1
1
Fa5/48 none

```

## Port Vlans allowed and active in management domain

```

Fa5/4 none
Fa5/5 none
Fa5/3 none
Fa5/4 none
Fa5/5 none
Fa5/6 none
Fa5/7 none
Fa5/8 500
Fa5/9 4-6,40,50,50,400,455,500,300,303-305,349-354,400,500,554,554,570,804-8
05,850,947,999,4005-4005
Fa5/40 none
Fa5/44 none
Fa5/45 none

```

```

1
1
1
Fa5/48 none

```

## Port Vlans in spanning tree forwarding state and not pruned

```

Fa5/4 none
Fa5/5 none
Fa5/3 none
Fa5/4 none
Fa5/5 none
Fa5/6 none
Fa5/7 none
Fa5/8 500
Fa5/9 4-6,40,50,50,400,455,500,300,303-305,349-354,400,500,554,554,570,804-8
05,850,947,999,4005-4005
Fa5/40 none
Fa5/44 none

```

```
1
1
1
```

```
Fa5/48 none
Router#
```

This example shows how to display the trunking information for active trunking ports:

```
Router# show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa5/9	desirable	n-isl	trunking	4

Port	Vlans allowed on trunk
Fa5/9	4-4005

Port	Vlans allowed and active in management domain
Fa5/9	4-6,40,50,50,400,455,500,300,303-305,349-354,400,500,554,554,570,804-805,850,947,999,4005-4005

Port	Vlans in spanning tree forwarding state and not pruned
Fa5/9	4-6,40,50,50,400,455,500,300,303-305,349-354,400,500,554,554,570,804-805,850,947,999,4005-4005

```
Router#
```

# show interfaces unidirectional

To display the operational state of an interface with a receive-only transceiver, use the **show interfaces unidirectional** command.

```
show interfaces [interface interface-number] unidirectional [module number]
```

Syntax Description		
<i>interface</i>	(Optional) Interface type; possible valid values are <b>gigabitethernet</b> and <b>tengigabitethernet</b> .	
<i>interface-number</i>	(Optional) Module and port number; see the “Usage Guidelines” section for valid values.	
<b>module</b> <i>number</i>	(Optional) Specifies the module number; see the “Usage Guidelines” section for valid values.	

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** If you do not specify a keyword, only information for trunking ports is displayed.

The *interface-number* designates the module and port number. Valid values depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 2 to 13 and valid values for the port number are from 1 to 48.

The **module** *number* keyword and argument designate the module number and limit the display to interfaces on the module. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values for the module number are from 2 to 13.

---

**Examples**

This example shows how to display the operational state of an interface with a receive-only transceiver:

```
Router# show interfaces gigabitethernet5/2 unidirectional
Unidirectional configuration mode: send only
Unidirectional operational mode: receive only
CDP neighbour unidirectional configuration mode: off
Router#
```

---

**Related Commands**

Command	Description
<a href="#">show interfaces status</a>	Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.
<a href="#">unidirectional</a>	Configures the software-based UDE.

# show interfaces vlan mapping

To display the status of a VLAN mapping on a port, use the **show interfaces vlan mapping** command.

**show interfaces** [*interface interface-number*] **vlan mapping**

Syntax Description	<i>interface</i>	(Optional) Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>vlan</b> , <b>pos</b> , <b>atm</b> , and <b>ge-wan</b> .
	<i>interface-number</i>	Module and port number; see the “Usage Guidelines” section for valid values.

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

**Command Modes** EXEC

Command History	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The *interface-number* designates the module and port number or the VLAN number. Valid values depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 1 to 13 and valid values for the port number are from 1 to 48.

**Examples** This example shows how to list all of the VLAN mappings that are configured on a port and indicate whether such mappings are enabled or disabled on the port:

```
Router# show interfaces gigabitethernet5/2 vlan mapping
State: enabled
Original VLAN Translated VLAN
-----
    4649             755
Router#
```

Related Commands	<b>Command</b>	<b>Description</b>
	<a href="#">show vlan mapping</a>	Registers a mapping of an 802.1Q VLAN to an ISL VLAN.
	<a href="#">switchport vlan mapping enable</a>	Enables VLAN mapping per switch port.

# show ip arp inspection

To display the status of DAI for a specific range of VLANs, use the **show ip arp inspection** command.

```
show ip arp inspection [{interfaces interface-name}] | {statistics [vlan vlan-range]}
```

Syntax Description	Parameter	Description
	<b>interfaces</b> <i>interface-name</i>	(Optional) Displays the trust state and the rate limit of ARP packets for the provided interface.
	<b>statistics</b>	(Optional) Displays statistics for the following types of packets that have been processed by this feature: forwarded, dropped, MAC validation failure, and IP validation failure.
	<b>vlan</b> <i>vlan-range</i>	(Optional) Displays the statistics for the selected range of VLANs.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** If you do not enter the **statistics** keyword, the configuration and operating state of DAI for the selected range of VLANs is displayed.

If you do not specify the interface name, the trust state and rate limit for all applicable interfaces in the system are displayed.

**Examples** This example shows how to display the statistics of packets that have been processed by DAI for VLAN 3:

```
Router# show ip arp inspection statistics vlan 3

Vlan      Forwarded      Dropped      DHCP Drops      ACL Drops
-----
3         34753         405407         405407          0

Vlan      DHCP Permits    ACL Permits    Source MAC Failures
-----
3         34753          0              0

Vlan      Dest MAC Failures  IP Validation Failures
-----
3         0                0

Router#
```

This example shows how to display the statistics of packets that have been processed by DAI for all active VLANs:

```
Router# show ip arp inspection statistics
```

Vlan	Forwarded	Dropped	DHCP Drops	ACL Drops
4	0	0	0	0
5	0	0	0	0
3	68355	550356	550356	0
4	0	0	0	0
400	0	0	0	0
404	0	0	0	0
4006	0	0	0	0
4007	0	0	0	0

Vlan	DHCP Permits	ACL Permits	Source MAC Failures
4	0	0	0
5	0	0	0
3	68355	0	0
4	0	0	0
400	0	0	0
404	0	0	0
4006	0	0	0
4007	0	0	0

Vlan	Dest MAC Failures	IP Validation Failures
4	0	0
5	0	0
3	0	0
4	0	0
400	0	0
404	0	0
4006	0	0
4007	0	0

```
Router#
```

This example shows how to display the configuration and operating state of DAI for VLAN 1:

```
Router# show ip arp inspection vlan 1
```

```
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
```

Vlan	Configuration	Operation	ACL Match	Static ACL
4	Enabled	Active		

Vlan	ACL Logging	DHCP Logging
4	Deny	Deny

```
Router#
```

This example shows how to display the trust state of interface Fa6/3:

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

Interface	Trust State	Rate (pps)	Burst Interval
Fa6/4	Untrusted	50	5

```
Router#
```

This example shows how to display the trust state of the interfaces on the switch:

```
Router# show ip arp inspection interfaces
Interface          Trust State      Rate (pps)
-----
Gi4/4              Untrusted        45
Gi4/5              Untrusted        45
Gi3/4              Untrusted        45
Gi3/5              Untrusted        45
Fa3/3              Trusted          None
Fa3/4              Untrusted        45
Fa3/5              Untrusted        45
Fa3/6              Untrusted        45
Fa3/7              Untrusted        45
Router#
```

Related Commands	Command	Description
	<a href="#">arp access-list</a>	Configures an ARP ACL for ARP inspection and QoS filtering and enters the ARP ACL configuration submenu.
	<a href="#">clear ip arp inspection log</a>	Clears the status of the log buffer.
	<a href="#">show ip arp inspection</a>	Displays the status of DAI for a specific range of VLANs.

# show ip arp inspection log

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

## show ip arp inspection log

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

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the current contents of the log buffer before and after the buffers are cleared:

```
Router# show ip arp inspection log
Total Log Buffer Size : 40
Syslog rate : 0 entries per 40 seconds1
```

Interface	Vlan	Sender MAC	Sender IP	Num of Pkts
Fa6/3	4	00051000510005	4141415	4 (45:05:55 UTC Fri Apr 55 5003)
Fa6/3	4	00051000510005	4141413	4 (45:05:55 UTC Fri Apr 55 5003)
Fa6/3	4	00051000510005	4141414	4 (45:05:55 UTC Fri Apr 55 5003)
Fa6/3	4	00051000510005	4141415	4 (45:05:55 UTC Fri Apr 55 5003)
Fa6/3	4	00051000510005	4141416	4 (45:05:55 UTC Fri Apr 55 5003)
Fa6/3	4	00051000510005	4141417	4 (45:05:55 UTC Fri Apr 55 5003)
Fa6/3	4	00051000510005	4141418	4 (45:05:55 UTC Fri Apr 55 5003)
Fa6/3	4	00051000510005	4141419	4 (45:05:55 UTC Fri Apr 55 5003)
Fa6/3	4	00051000510005	41414140	4 (45:05:55 UTC Fri Apr 55 5003)
Fa6/3	4	00051000510005	41414144	4 (45:05:55 UTC Fri Apr 55 5003)
--	--	--	--	5 (45:05:55 UTC Fri Apr 55 5003)

```
Router#
```

This example shows how to clear the buffer with the **clear ip arp inspection log** command:

```
Router# clear ip arp inspection log
Router# show ip arp inspection log
Total Log Buffer Size : 40
Syslog rate : 0 entries per 40 seconds1
No entries in log buffer1
Router#
```

Related Commands	Command	Description
	<b>clear ip arp inspection log</b>	Clears the status of the log buffer.
	<b>show ip arp inspection log</b>	Shows the status of the log buffer.

# show ip auth-proxy watch-list

To display the information about the authentication proxy watch list, use the **show ip auth-proxy watch-list** command.

## show ip auth-proxy watch-list

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

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the information about the authentication proxy watch list:

```
Router# show ip auth-proxy watch-list
Authentication Proxy Watch-list is enabled
Watch-list expiry timeout is 5 minutes
Total number of watch-list entries: 3

Source IP      Type           Violation-count
45101015      MAX_RETR\     MAX_LIMIT
45101013      TCP_NO_DATA   MAX_LIMIT
4151314       CFGED         N/A

Total number of watch-listed users: 3
Router#
```

Related Commands	Command	Description
	<a href="#">clear ip auth-proxy watch-list</a>	Deletes a single watch-list entry or all watch-list entries.
	<a href="#">ip auth-proxy max-login-attempts</a>	Limits the number of login attempts at a firewall interface.
	<a href="#">ip auth-proxy watch-list</a>	Enables and configures an authentication proxy watch list.

# show ipc

To display IPC information, use the **show ipc** command.

**show ipc {nodes | ports [open] | queue | status}**

Syntax Description	nodes	Displays the participating nodes.
	ports	Displays the local IPC ports.
	open	(Optional) Displays the open ports only.
	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** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display participating nodes:

```
Router# show ipc nodes
There are 66 nodes in this IPC realm1
  ID      Type      Name
 5540000 Local      Card33
 5000000 ICC        Card0
 5040000 ICC        Card4
 5050000 ICC        Card5
 5040000 ICC        Card4

<111 output truncated 111>

 53E0000 ICC        Card65
 53F0000 ICC        Card63
 40000 ICC        IPC Master
Router#
```

This example shows how to display local IPC ports:

```
Router# show ipc ports
There are 6 ports defined1

Port ID      Type      Name
554000014   unicast   Card33:]one
554000015   unicast   Card33:Echo
554000013   unicast   Card33:Control
554000014   unicast   Remote TT\ Server Port
4000013     unicast   IPC Master:Control
```

```

554000015      unknown      Card33:Request
      port_index = 0  seat_id = 0x40000  last sent = 0  last heard = 4458
      port_index = 4  seat_id = 0x40000  last sent = 0  last heard = 0
Router#

```

This example shows how to display open IPC ports:

```

Router# show ipc ports open
There are 4 ports defined1

Port ID      Type      Name
4000017      unicast   Unknown
      port_index = 0  last sent = 5      last heard = 0

4000018      unicast   Unknown
      port_index = 0  last sent = 0      last heard = 0

4000019      unicast   Unknown
      port_index = 0  last sent = 47753  last heard = 0
      port_index = 4  last sent = 0      last heard = 0
Router#

```

This example shows how to display the contents of the IPC-retransmission queue:

```

Router# show ipc queue
There are 0 IPC messages waiting for acknowledgement in the transmit queue1
There are 0 IPC messages waiting for a response1
There are 0 IPC messages waiting for additional fragments1
There are 5 messages currently in use by the system1
Router#

```

This example shows how to display the status of the local IPC server:

```

Router# show ipc status
IPC System Status:

This processor is a slave server1

4000 IPC message headers in cache
377053 messages in, 593433 out, 540699 delivered to local port,
83655 acknowledgements received, 83870 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 timeouts1
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, 0 failed opens, 0 hardware errors
No regular dropping of IPC output packets for test purposes
Router#

```

# show ip cache flow

To display a summary of the NetFlow cache-flow entries, use the **show ip cache flow** command.

**show ip cache flow** [**aggregation type** [**module num**]]

<b>Syntax Description</b>	<b>aggregation type</b> (Optional) Displays the configuration of a particular aggregation cache; see the “Usage Guidelines” section for valid values.
	<b>module num</b> (Optional) Displays information about a specific module.

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

**Command Modes** EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Valid values for **aggregation type** are as follows:

- **as**—AS aggregation cache
- **destination-prefix**—Destination-prefix aggregation cache
- **prefix**—Source/destination-prefix aggregation cache
- **protocol-port**—Protocol and port aggregation cache
- **source-prefix**—Source-prefix aggregation cache

If you enter the **show ip cache flow aggregation** command without the **module num**, the software-switched aggregation cache on the route processor (RP) is displayed.

**Examples** This example shows how to display a summary of the NetFlow cache-flow entries:

```
Router# show ip cache flow
IP packet size distribution (0 total packets):
 4-35 64 96 458 460 495 554 556 588 350 355 384 446
448
480
 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000
1000 1000

 545 544 576 4054 4536 5048 5560 3075 3584 4096 4608
1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000

IP Flow Switching Cache, 0 bytes
0 active, 0 inactive, 0 added
0 ager polls, 0 flow alloc failures
Active flows timeout in 30 minutes
```

## show ip cache flow

```

Inactive flows timeout in 45 seconds
last clearing of statistics never
Protocol Total Flows Packets Bytes Packets Active(Sec)
Idle(Sec)
----- Flows /Sec /Flow /Pkt /Sec /Flow
/Flow

SrcIf SrcIPAddress DstIf DstIPAddress Pr SrcP
DstP
Pkts

Displaying Hardware entries in Module 7
SrcIf SrcIPAddress DstIPAddress Pr SrcP
DstP Pkts
Fa5/44 441414138 45141415 udp 63
63 986796
Fa5/44 441414139 45141415 udp 63
63 986796
Fa5/44 441414140 45141415 udp 63
63 986796
Fa5/44 441414144 45141415 udp 63
63 986796
Fa5/44 441414145 45141415 udp 63
63 986796
Fa5/44 441414143 45141415 udp 63
63 986796
Fa5/44 441414144 45141415 udp 63
63 986796
Fa5/44 441414145 45141415 udp 63
63 986796
Fa5/44 441414146 45141415 udp 63
63 986796
Fa5/44 441414147 45141415 udp 63
63 986796
Fa5/44 441414148 45141415 udp 63
63 986796
Router#

```

This example shows how to display the information about a destination-prefix aggregation cache for a specific module:

```

Router# show ip cache flow aggregation destination-prefix module 1
IPFLOW_DST_PREFIX_AGGREGATION records and statistics for module :4
IP Flow Switching Cache, 578544 bytes
 5 active, 4094 inactive, 6 added
 536 ager polls, 0 flow alloc failures
Active flows timeout in 30 minutes
Inactive flows timeout in 45 seconds

Dst If          Dst Prefix      Msk AS    Flows  Pkts B/Pk  Active
Gi7/9           9141010         /46 0       3003   45M   64   469918
Gi7/40          44141010        /46 0       3000   9873K 64   469918
Router#

```

Table 2-39 describes the **show ip cache flow** command output fields.

**Table 2-39** *show ip cache flow Command Output Fields—Packet Size Distribution*

Field	Description
IP packet size distribution	Two lines below this banner that show the percentage distribution of packets by size range. In this display, 55.4% of the packets fall in the size range of 33 to 64 bytes.

Table 2-40 describes the fields in the flow-switching cache lines of the output.

**Table 2-40** *show ip cache flow Command Output Fields—Flow-Switching Cache*

Field	Description
bytes	Number of bytes of memory that the NetFlow cache uses.
active	Number of active flows in the NetFlow cache at the time this command was entered.
inactive	Number of flow buffers that are allocated in the NetFlow cache but are not currently assigned to a specific flow at the time this command was entered.
added	Number of flows that were created since the start of the summary period.
ager polls	Number of times that the NetFlow code looked at the cache to expire entries (used by Cisco for diagnostics only).
flow alloc failures	Number of times that the NetFlow code tried to allocate a flow but could not.
Exporting flows to	IP address and UDP port number of the workstation to which flows are exported.
Exporting using source interface	Interface type that is used as the source IP address.
Version 5 flow records, peer-as	Exported packets that use version 5 format and the export statistics that include the peer AS for the source and destination. The number of records stored in the datagram is between 1 and 30 for version 5.
Active flows timeout in	Timeout period for active flows in the NetFlow cache.
flows exported in udp datagrams	Total number of flows that are exported and the total number of UDP datagrams that are used to export the flows to the workstation.
failed	Number of flows that could not be exported by the router because of output interface limitations.
last clearing of statistics	Standard time output (hh:mm:ss) since the <b>clear ip flow stats</b> command was executed. This time output changes to hours and days after the time exceeds 24 hours.

Table 2-41 describes the fields in the NetFlow activity by protocol lines of the output.

**Table 2-41** *show ip cache flow Command Output Fields—NetFlow Activity by Protocol*

Field	Description
Protocol	IP protocol and the well-known port number as described in RFC 1340.
Total Flows	Number of flows for this protocol since the last time that the statistics were cleared.
Flows/Sec	Average number of flows for this protocol seen per second; equal to total flows/number of seconds for this summary period.
Packets/Flow	Average number of packets observed for the flows seen for this protocol. Equal to total packets for this protocol/number of flows for this protocol for this summary period.

**Table 2-41** *show ip cache flow Command Output Fields—NetFlow Activity by Protocol (continued)*

Field	Description
Bytes/Pkt	Average number of bytes observed for the packets seen for this protocol. Equal to total bytes for this protocol/total number of packets for this protocol for this summary period.
Packets/Sec	Average number of packets for this protocol per second. Equal to total packets for this protocol/total number of seconds for this summary period.
Active(Sec)/Flow w	Sum of all the seconds from the first packet to the last packet of an expired flow (for example, TCP FIN, time-out, and so forth) in seconds/total flows for this protocol for this summary period.
Idle(Sec)/Flow	Sum of all the seconds from the last packet seen in each nonexpired flow for this protocol until the time this command was entered in seconds/total flows for this summary period.

Table 2-42 describes the fields in the current flow lines of the output.

**Table 2-42** *show ip cache flow Command Output Fields—Current Flow*

Field	Description
SrcIf	Internal port name for the source interface.
SrcIPAddress	Source-IP address for this flow.
DstIf	Router internal port name for the destination interface.
DstIPAddress	Destination-IP address for this flow.
Pr	IP protocol; for example, 6=TCP, 17=UDP, .... as defined in RFC 1340.
SrcP	Source port address, TCP/UDP “well known” port number, as defined in RFC 1340.
DstP	Destination-port address, TCP/UDP “well known” port number, as defined in RFC 1340.
Pkts	Number of packets observed for this flow.
B/Pkt	Average observed number of bytes per packet for this flow.
Active	Number of seconds between first and last packet of a flow.

**Related Commands**

Command	Description
<b>ip flow-aggregation cache</b>	Creates a flow-aggregation cache and enters the aggregation cache configuration mode.
<b>ip flow-cache entries</b>	Changes the number of entries that are maintained in the NetFlow cache.
<b>clear ip flow stats</b>	Clears the NetFlow-switching statistics.

# show ip cache verbose flow

To display a detailed summary of NetFlow statistics, use the **show ip cache verbose flow** command.

## show ip cache verbose flow

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

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Use the **show ip cache verbose flow** command to display the flow record fields in the NetFlow cache in addition to the fields that are displayed with the **show ip cache flow** command. The values in the additional fields that are shown depend on the NetFlow features that are enabled and the flags that are set in the flow.



**Note** The flags and the fields displayed vary from flow to flow.

When you configure the MPLS-aware NetFlow feature, you can use the **show ip cache verbose flow** command to display both the IP and MPLS portions of the MPLS flows in the NetFlow cache on a router module. To display only the IP portion of the flow record in the NetFlow cache when MPLS-aware NetFlow is configured, use the **show ip cache flow** command.

**Examples** This example shows how to display a detailed summary of NetFlow statistics:

```
Router# show ip cache verbose flow
IP packet size distribution (4094508 total packets):
  4-35  64  96  458  460  495  554  556  588  350  355  384  446  448  480
 1000 4100 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000

      545  544  576 4054 4536 5048 5560 3075 3584 4096 4608
      1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000

IP Flow Switching Cache, 4456704 bytes
 5 active, 65534 inactive, 5 added
 598 ager polls, 0 flow alloc failures
 Active flows timeout in 30 minutes
 Inactive flows timeout in 45 seconds
IP Sub Flow Cache, 570600 bytes
 4 active, 46380 inactive, 4 added, 5 added to flow
 0 alloc failures, 0 force free
```

## show ip cache verbose flow

```

4 chunk, 4 chunk added
last clearing of statistics never
Protocol      Total      Flows      Packets Bytes  Packets Active (Sec) Idle (Sec)
-----      -
              Flows      /Sec       /Flow  /Pkt   /Sec     /Flow     /Flow

SrcIf      SrcIPAddress  DstIf      DstIPAddress  Pr TOS Flgs Pkts
Port Msk AS  Port Msk AS  NextHop      B/Pk Active
IPM: OPkts  OBytes

SrcIf      SrcIPAddress  DstIf      DstIPAddress  Pr TOS Flgs Pkts
Port Msk AS  Port Msk AS  NextHop      B/Pk Active
IPM: OPkts  OBytes
Fa5/44      44141415     Fa5/45     45141415     06 5B 00    554K
0000 /46 0    0000 /46 0    45141415     46    44917
FO: 4
Fa5/44      44141413     Fa5/45     45141415     06 5B 00    553K
0000 /46 0    0000 /46 0    45141415     46    45014
FO: 4

Displaying Hardware entries in Module 7
 SrcIf      SrcIPAddress  DstIPAddress  Pr      SrcP      DstP
Pkts
--          0101010     0101010     0      0      0      3

Router#

```

Table 2-43 describes the fields shown in the NetFlow cache lines of the display.

**Table 2-43 show ip cache verbose flow Field Descriptions in the NetFlow Cache Display**

Field	Description
bytes	Number of bytes of memory that are used by the NetFlow cache.
active	Number of active flows in the NetFlow cache at the time this command was entered.
inactive	Number of flow buffers that are allocated in the NetFlow cache but that are not assigned to a specific flow at the time this command is entered.
added	Number of flows that were created since the start of the summary period.
ager polls	Number of times that the NetFlow code caused entries to expire (used by Cisco for diagnostics only).
flow alloc failures	Number of times that the NetFlow code tried to allocate a flow but could not.
last clearing of statistics	Standard time output (hh:mm:ss) since the <b>clear ip flow stats</b> privileged EXEC command was last executed. This time output changes to hours and days after the time exceeds 24 hours.

Table 2-44 describes the fields shown in the activity by the protocol lines of the display.

**Table 2-44** *show ip cache verbose flow Field Descriptions in Activity By Protocol Display*

Field	Description
Protocol	IP protocol and port number. (Go to <a href="http://www.iana.org">http://www.iana.org</a> , <i>Protocol Assignment Number Services</i> , for the latest RFC values.) <b>Note</b> Only a small subset of all protocols is displayed.
Total Flows	Number of flows for this protocol since the last time statistics were cleared.
Flows/Sec	Average number of flows for this protocol per second; equal to the total flows divided by the number of seconds for this summary period.
Packets/Flow	Average number of packets for the flows for this protocol; equal to the total packets for this protocol divided by the number of flows for this protocol for this summary period.
Bytes/Pkt	Average number of bytes for the packets for this protocol; equal to the total bytes for this protocol divided by the total number of packets for this protocol for this summary period.
Packets/Sec	Average number of packets for this protocol per second; equal to the total packets for this protocol divided by the total number of seconds for this summary period.
Active(Sec)/Flow	Number of seconds from the first packet to the last packet of an expired flow (for example, TCP connection close request [FIN], timeout, and so on) divided by the total flows for this protocol for this summary period.
Idle(Sec)/Flow	Number of seconds observed from the last packet in each nonexpired flow for this protocol until the time at which this command was entered divided by the total flows for this protocol for this summary period.

Table 2-45 describes the fields in the NetFlow record lines of the display.

**Table 2-45** *show ip cache verbose flow Field Descriptions in NetFlow Record Display*

Field	Description
SrcIf	Interface on which the packet was received.
Port Msk AS	Source port number (displayed in hexadecimal format), IP address mask, and autonomous system number. This field is always set to 0 in MPLS flows.
SrcIPAddress	IP address of the device that transmitted the packet.
DstIf	Interface from where the packet was transmitted.
Port Msk AS	Destination port number (displayed in hexadecimal format), IP address mask, and autonomous system. This field is always set to 0 in MPLS flows.
DstIPAddress	IP address of the destination device.

**Table 2-45** show ip cache verbose flow Field Descriptions in NetFlow Record Display (continued)

Field	Description
NextHop	BGP next-hop address. This field is always set to 0 in the MPLS flows.
Pr	IP protocol port number, displayed in hexadecimal format. (Go to <a href="http://www.iana.org">http://www.iana.org</a> , <i>Protocol Assignment Number Services</i> , for the latest RFC values.)
TOS	Type of service, displayed in hexadecimal format.
B/Pk	Average number of bytes that are observed for the packets seen for this protocol.
Flgs	TCP flags, shown in hexadecimal format (result of bitwise OR of TCP flags from all packets in the flow).
Pkts	Number of packets in this flow.
Active	Time the flow has been active.
FO	Fragment offset.

**Related Commands**

Command	Description
<b>ip flow-cache mpls label positions</b>	Enables MPLS-aware NetFlow.
<b>ip route-cache flow</b>	Enables NetFlow switching for IP routing.
<b>show ip cache flow</b>	Displays a summary of the NetFlow cache-flow entries.

# show ip cef epoch

To display the epoch information for the adjacency table and all FIB tables, use the **show ip cef epoch** command.

## show ip cef epoch

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

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** These **show** commands also display the epoch information for the following:

- **show ip cef summary**—Displays the table epoch for a specific FIB table.
- **show ip cef detail**—Displays the epoch value for each entry of a specific FIB table.
- **show adjacency summary**—Displays the adjacency table epoch.
- **show adjacency detail**—Displays the epoch value for each entry of the adjacency table.

**Examples** This example shows how to display epoch information:

```
Router# show ip cef epoch
CEF epoch information:

Table:Default-table
  Table epoch:5 (464 entries at this epoch)

Adjacency table
  Table epoch:4 (33 entries at this epoch)
```

This example shows the output after you clear the epoch table and increment the epoch number:

```
Router# show ip cef epoch
CEF epoch information:

Table:Default-table
  Table epoch:5 (464 entries at this epoch)

Adjacency table
  Table epoch:4 (33 entries at this epoch)
```

## ■ show ip cef epoch

```

Router# clear ip cef epoch full
Router# show ip cef epoch
CEF epoch information:

Table:Default-table
  Table epoch:3 (464 entries at this epoch)

Adjacency table
  Table epoch:5 (33 entries at this epoch)
Router#

```

## Syntax Description

Command	Description
<b>clear ip cef epoch full</b>	Begins a new epoch and increments the epoch number for all tables (including the adjacency table).
<b>show ip cef</b>	Displays entries in the FIB or displays a summary of the FIB.

# show ip cef inconsistency

To display the IP CEF inconsistencies, use the **show ip cef inconsistency** command.

```
show ip cef [vrf vrf-name] inconsistency [records [detail]]
```

Syntax Description	
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VRF instance.
<b>records</b>	(Optional) Displays all recorded inconsistencies.
<b>detail</b>	(Optional) Displays the detailed information for each CEF table entry.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command displays the recorded IP CEF inconsistency records found by the lc-detect, scan-rp, scan-rib, and scan-lc detection mechanisms.

You can configure the IP CEF-prefix consistency-detection mechanisms using the **ip cef table consistency-check** command.

**Examples** This example shows how to display the recorded CEF inconsistency records:

```
Router# show ip cef inconsistency
Table consistency checkers (settle time 65s)
  lc-detect:running
    0/0/0 queries sent/ignored/received
  scan-lc:running [400 prefixes checked every 60s]
    0/0/0 queries sent/ignored/received
  scan-rp:running [400 prefixes checked every 60s]
    0/0/0 queries sent/ignored/received
  scan-rib:running [4000 prefixes checked every 60s]
    0/0/0 queries sent/ignored/received
Inconsistencies:0 confirmed, 0/46 recorded
```

Table 2-46 describes the fields shown in the display.

**Table 2-46** *show ip cef inconsistency* Field Descriptions

Field	Description
settle time	Time after a recorded inconsistency is confirmed.
lc-detect running	Consistency checker lc-detect is running.
0/0/0 queries	Number of queries sent, ignored, and received.
Inconsistencies:	Number of inconsistencies confirmed and recorded. The maximum number of inconsistency records to be recorded is 16.

#### Related Commands

Command	Description
<b>clear ip cef inconsistency</b>	Clears the statistics and records for the CEF-consistency checker.

# show ip cef summary

To display a summary of the IP CEF table, use the **show ip cef summary** command.

## **show ip cef summary**

<b>Syntax Description</b>	This command has no keywords and arguments.
---------------------------	---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Examples</b>	This example shows how to display a summary of the IP CEF table:
-----------------	--

```
Router# show ip cef summary
IP Distributed CEF with switching (Table Version 55), flags=0x0
 54 routes, 0 reresolve, 0 unresolved (0 old, 0 new), peak 4
 54 leaves, 46 nodes, 49496 bytes, 36 inserts, 45 invalidations
 0 load sharing elements, 0 bytes, 0 references
universal per-destination load sharing algorithm, id 5463EC45
3(0) CEF resets, 0 revisions of existing leaves
Resolution Timer: Exponential (currently 4s, peak 4s)
 0 in-place/0 aborted modifications
refcounts: 4377 leaf, 4355 node

Table epoch: 0 (54 entries at this epoch)

Adjacency Table has 9 adjacencies
Router#
```

# show ip cef vlan

To display the information about the IP CEF VLAN interface status, the configuration, and the prefixes for a specific interface, use the **show ip cef vlan** command.

**show ip cef vlan *vlan-id* [detail]**

Syntax Description	<i>vlan-id</i>	VLAN number; valid values are from 1 to 4094.
	<b>detail</b>	(Optional) Displays the detailed information about the IP CEF VLAN interface.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the prefixes for a specific VLAN:

```
Router> show ip cef vlan 1003
Prefix           Next Hop           Interface
0101010/0        47515015514        FastEthernet3/3
0101010/35       receive
40171010/46      47515015514        FastEthernet3/3
4014614810/53    47515015514        FastEthernet3/3
Router>
```

This example shows how to display detailed IP CEF information for a specific VLAN:

```
Router> show ip cef vlan 1003 detail
IP Distributed CEF with switching (Table Version 5364), flags=0x0
 4383 routes, 0 reresolve, 0 unresolved (0 old, 0 new)
 4383 leaves, 504 nodes, 380535 bytes, 5375 inserts, 989 invalidations
 0 load sharing elements, 0 bytes, 0 references
 universal per-destination load sharing algorithm, id 9B6C9853
 3 CEF resets, 0 revisions of existing leaves
  refcounts: 54576 leaf, 54745 node
Adjacency Table has 5 adjacencies
Router>
```

# show ip dhcp relay information trusted-sources

To list all the configured trusted interfaces, use the **show ip dhcp relay information trusted-sources** command.

## show ip dhcp relay information trusted-sources

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

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display a list of all the configured trusted interfaces:

```
Router# show ip dhcp relay information trusted-sources
List of trusted sources of relay agent information option:
Vlan60          Vlan65
Router#
```

Related Commands	Command	Description
	<a href="#">ip dhcp relay information option trust-all</a>	Enables all the interfaces as trusted sources of the DHCP relay-agent information option.
	<a href="#">ip dhcp relay information trust</a>	Enables an interface as a trusted source of the DHCP relay-agent information.

# show ip dhcp snooping

To display the DHCP snooping configuration, use the **show ip dhcp snooping** command.

**show ip dhcp snooping [statistics [detail]]**

Syntax Description	
<b>statistics</b>	(Optional) Displays statistics information about DHCP snooping.
<b>detail</b>	(Optional) Displays the detailed information about DHCP snooping.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the DHCP snooping configuration:

```
Router# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
5 40
Insertion of option 85 is enabled
Interface           Trusted      Rate limit (pps)
-----
FastEthernet6/44   no          40
FastEthernet6/36   yes         50
Router#
```

This example shows how to display the DHCP snooping statistics information:

```
Router# show ip dhcp snooping statistics
Packets Processed by DHCP Snooping          = 0
Packets Dropped Because
  IDB not known                             = 0
  Queue full                                = 0
  Interface is in errdisabled                = 0
  Rate limit exceeded                       = 0
  Received on untrusted ports               = 0
  Nonzero giaddr                             = 0
  Source mac not equal to chaddr             = 0
  No binding entry                           = 0
  Insertion of opt85 fail                    = 0
  Unknown packet                             = 0
  Interface Down                             = 0
  Unknown output interface                   = 0
Router#
```

This example shows how to display detailed DHCP snooping statistics information:

```
Router# show ip dhcp snooping statistics detail
Packets Forwarded                          = 0
```

```

Packets Dropped = 0
Packets Dropped From untrusted ports = 0
Router#

```

Related Commands	Command	Description
	<b>clear ip dhcp snooping</b>	Clears the IP DHCP table entries.
	<b>ip dhcp snooping</b>	Globally enables DHCP snooping.
	<b>ip dhcp snooping binding</b>	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
	<b>ip dhcp snooping database</b>	Configures the DHCP snooping database.
	<b>ip dhcp snooping information option</b>	Enables DHCP option 82 data insertion.
	<b>ip dhcp snooping limit rate</b>	Configures the number of the DHCP messages that an interface can receive per second.
	<b>ip dhcp snooping packets</b>	Enables DHCP snooping on the tunnel interface.
	<b>ip dhcp snooping verify mac-address</b>	Verifies that the source MAC address in a DHCP packet matches the client hardware address on an untrusted port.
	<b>ip dhcp snooping vlan</b>	Enables DHCP snooping on a VLAN or a group of VLANs.
	<b>show ip dhcp snooping binding</b>	Displays the DHCP snooping binding entries.
	<b>show ip dhcp snooping database</b>	Displays the status of the DHCP snooping database agent.

# 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]
[interface interface interface-num]
```

Syntax Description		
<i>ip-address</i>	(Optional) IP address for the binding entries.	
<i>mac-address</i>	(Optional) MAC address for the binding entries.	
<b>vlan</b> <i>vlan</i>	(Optional) Specifies a valid VLAN number; valid values are from 1 to 4094.	
<b>interface</b> <i>interface</i>	(Optional) Specifies the interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , and <b>tengigabitethernet</b> .	
<i>interface-num</i>	Module and port number.	

**Defaults** If no argument is specified, the switch displays the entire DHCP snooping binding table.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** DHCP snooping is enabled on a VLAN only if both the global snooping and the VLAN snooping are enabled.

**Examples** This example shows how to display the DHCP snooping binding entries for a switch:

```
Router# show ip dhcp snooping binding
```

```
MacAddress      IP Address      Lease (seconds)  Type              VLAN      Interface
-----
00001040010504  40101014       4600             dhcp-snooping    400      FastEthernet3/4
Router#
```

This example shows how to display an IP address for DHCP snooping binding entries:

```
Router# show ip dhcp snooping binding 172.100.101.102
```

```
MacAddress      IP Address      Lease (seconds)  Type              VLAN      Interface
-----
00001040010504  475140014041405  4600             dhcp-snooping    400      FastEthernet3/4
Router#
```

This example shows how to display the MAC address for the DHCP snooping binding entries:

```
Router# show ip dhcp snooping binding 55.5.5.2 0002.b33f.3d5f
```

```
MacAddress      IpAddress      Lease(sec)    Type           VLAN  Interface
-----
00:05:B3:3F:3D:5F  55151515      495           dhcp-snooping  99   FastEthernet6/36
Router#
```

This example shows how to display the DHCP snooping binding entries' MAC address for a specific VLAN:

```
Router# show ip dhcp snooping binding 55.5.5.2 0002.b33f.3d5f vlan 99
```

```
MacAddress      IpAddress      Lease(sec)    Type           VLAN  Interface
-----
00:05:B3:3F:3D:5F  55151515      479           dhcp-snooping  99   FastEthernet6/36
Router#
```

This example shows how to display the dynamic DHCP snooping binding entries:

```
Router# show ip dhcp snooping binding dynamic
```

```
MacAddress      IP Address      Lease (seconds)    Type           VLAN  Interface
-----
00001040010504  40101014       4600              dhcp-snooping  400   FastEthernet3/4
Router#
```

This example shows how to display the DHCP snooping binding entries on VLAN 100:

```
Router# show ip dhcp snooping binding vlan 100
```

```
MacAddress      IP Address      Lease (seconds)    Type           VLAN  Interface
-----
00001040010504  40101014       4600              dhcp-snooping  400   FastEthernet3/4
Router#
```

This example shows how to display the DHCP snooping binding entries on Ethernet interface 0/1:

```
Router# show ip dhcp snooping binding interface fastethernet3/1
```

```
MacAddress      IP Address      Lease (seconds)    Type           VLAN  Interface
-----
00001040010504  40101014       4600              dhcp-snooping  400   FastEthernet3/4
Router#
```

Table 2-47 describes the fields in the **show ip dhcp snooping** command output.

**Table 2-47 show ip dhcp snooping Command Output**

Field	Description
Mac Address	Client hardware MAC address.
IP Address	Client IP address assigned from the DHCP server.
Lease (seconds)	IP address lease time.
Type	Binding type; statically configured from CLI or dynamically learned.
VLAN	VLAN number of the client interface.
Interface	Interface that connects to the DHCP client host.

## ■ show ip dhcp snooping binding

Related Commands	Command	Description
	<b>ip dhcp snooping</b>	Globally enables DHCP snooping.
	<b>ip dhcp snooping binding</b>	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
	<b>ip dhcp snooping database</b>	Configures the DHCP snooping database.
	<b>ip dhcp snooping information option</b>	Enables DHCP option 82 data insertion.
	<b>ip dhcp snooping limit rate</b>	Configures the number of the DHCP messages that an interface can receive per second.
	<b>ip dhcp snooping packets</b>	Enables DHCP snooping on the tunnel interface.
	<b>ip dhcp snooping verify mac-address</b>	Verifies that the source MAC address in a DHCP packet matches the client hardware address on an untrusted port.
	<b>ip dhcp snooping vlan</b>	Enables DHCP snooping on a VLAN or a group of VLANs.
	<b>show ip dhcp snooping</b>	Displays the DHCP snooping configuration.
	<b>show ip dhcp snooping database</b>	Displays the status of the DHCP snooping database agent.

# 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]

<b>Syntax Description</b>	<b>detail</b> (Optional) Provides additional operating state and statistics information.
---------------------------	--

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

**Command Modes** Privileged EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the DHCP snooping database:

```
Router# show ip dhcp snooping database
Agent URL :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded1

Total Attempts      :          0  Startup Failures :          0
Successful Transfers :          0  Failed Transfers :          0
Successful Reads     :          0  Failed Reads     :          0
Successful Writes    :          0  Failed Writes    :          0
Media Failures       :          0

Router#
```

This example shows how to view additional operating statistics:

```
Router# show ip dhcp snooping database detail
Agent URL : tftp://40141414/directory/file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 7 (00:00:07)
Abort Timer Expiry : Not Running

Last Succeeded Time : None
```

## ■ show ip dhcp snooping database

```

Last Failed Time : 47:44:55 UTC Sat Jul 7 5004
Last Failed Reason : Unable to access URL1

Total Attempts      :      54  Startup Failures :      0
Successful Transfers :      0  Failed Transfers :     54
Successful Reads    :      0  Failed Reads    :      0
Successful Writes   :      0  Failed Writes   :     54
Media Failures     :      0

First successful access: Read

Last ignored bindings counters :
Binding Collisions :      0  Expired leases :      0
Invalid interfaces :      0  Unsupported vlans :     0
Parse failures     :      0
Last Ignored Time : None

Total ignored bindings counters:
Binding Collisions :      0  Expired leases :      0
Invalid interfaces :      0  Unsupported vlans :     0
Parse failures     :      0

Router#

```

## Related Commands

Command	Description
<a href="#">ip dhcp snooping</a>	Globally enables DHCP snooping.
<a href="#">ip dhcp snooping binding</a>	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
<a href="#">ip dhcp snooping database</a>	Configures the DHCP snooping database.
<a href="#">ip dhcp snooping information option</a>	Enables DHCP option 82 data insertion.
<a href="#">ip dhcp snooping limit rate</a>	Configures the number of the DHCP messages that an interface can receive per second.
<a href="#">ip dhcp snooping packets</a>	Enables DHCP snooping on the tunnel interface.
<a href="#">ip dhcp snooping verify mac-address</a>	Verifies that the source MAC address in a DHCP packet matches the client hardware address on an untrusted port.
<a href="#">ip dhcp snooping vlan</a>	Enables DHCP snooping on a VLAN or a group of VLANs.
<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.
<a href="#">show ip dhcp snooping binding</a>	Displays the DHCP snooping binding entries.

# show ip flow-export

To display the information about the software-switched flows for the data export, including the main cache and all other enabled caches, use the **show ip flow export** command.

**show ip flow export** [**template** | **verbose**]

Syntax Description	template	(Optional) Displays export template statistics information.
	verbose	(Optional) Displays verbose export statistics information.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the information about the software-switched flows for NDE:

```
Router# show ip flow export
Flow export v4 is disabled for main cache
Version 4 flow records
 0 flows exported in 0 udp datagrams
 0 flows failed due to lack of export packet
 0 export packets were sent up to process level
 0 export packets were dropped due to no fib
 0 export packets were dropped due to adjacency issues
 0 export packets were dropped due to fragmentation failures
 0 export packets were dropped due to encapsulation fixup failures
 0 export packets were dropped enqueueing for the RP
 0 export packets were dropped due to IPC rate limiting
Router#
```

This example shows how to display export template statistics information:

```
Router# show ip flow export template
No Template export information
No Option Templates exist
  Template Options Flag = 0
  Total number of Templates added = 0
  Total active Templates = 0
  Flow Templates active = 0
  Flow Templates added = 0
  Option Templates active = 0
  Option Templates added = 0
  Template ager polls = 0
  Option Template ager polls = 0
Main cache version 9 export is disabled
Router#
```

This example shows how to display export verbose statistics information:

```
Router# show ip flow export verbose
Flow export v4 is disabled for main cache
  Version 4 flow records
    0 flows exported in 0 udp datagrams
    0 flows failed due to lack of export packet
    0 export packets were sent up to process level
    0 export packets were dropped due to no fib
    0 export packets were dropped due to adjacency issues
    0 export packets were dropped due to fragmentation failures
    0 export packets were dropped due to encapsulation fixup failures
    0 export packets were dropped enqueueing for the RP
    0 export packets were dropped due to IPC rate limiting
Router#
```

#### Related Commands

Command	Description
<b>clear adjacency</b>	Clears the CEF adjacency table.
<b>ip flow-aggregation cache</b>	Creates a flow-aggregation cache and enters the aggregation cache configuration mode.

# show ip igmp groups

To display the multicast groups with receivers that are directly connected to the router and that were learned through IGMP, use the **show ip igmp groups** command.

```
show ip igmp [vrf vrf-name] groups [group-name | group-address | interface-type
interface-number] [detail]
```

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
<i>group-name</i>	(Optional) Name of the multicast group as defined in the DNS hosts table.	
<i>group-address</i>	(Optional) Address of the multicast group in four-part, dotted-decimal notation.	
<i>interface-type</i>	(Optional) Interface type.	
<i>interface-number</i>	(Optional) Interface number.	
<b>detail</b>	(Optional) Provides a detailed description of the sources that are known through IGMP Version 3 (IGMPv3), IGMP v3lite, or URL Rendezvous Directory (URD).	

Command Modes	
	EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Usage Guidelines	
	If you omit all optional arguments and keywords, the <b>show ip igmp groups</b> command displays all directly connected multicast groups by group address, interface type, and interface number.

Examples	
	This example shows how to display output from the <b>show ip igmp groups</b> command:

```
Router# show ip igmp groups
```

```
IGMP Connected Group Membership
Group Address      Interface      Uptime        Expires       Last Reporter
539155515551554   Ethernet3/4    4w0d          00:05:49     47515415001459
5541014140         Ethernet3/4    4w0d          00:05:45     475154150014
5541014140         Ethernet3/3    4w0d          never         47514615441554
554101414         Ethernet3/4    4w0d          00:05:44     4751541500144
554191915         Ethernet3/4    4w0d          00:05:40     47515415001455
535141414         Ethernet3/4    5d54h         stopped      47515415001506
```

This example shows how to display output from the **show ip igmp groups** command with the *group-address* argument and **detail** keyword:

```
Router# show ip igmp groups 232.1.1.1 detail
```

```
Interface:      Ethernet3/5
Group:          535141414
```

## ■ show ip igmp groups

```

Uptime:          04:58:58
Group mode:      INCLUDE
Last reporter:   401014491433
CSR Grp Exp:     00:05:38
Group source list: (C - Cisco Src Report, U - URD, R - Remote)
  Source Address  Uptime    v3 Exp    CSR Exp    Fwd  Flags
  475146154414   04:58:58  stopped   00:05:34  \es  C

```

Table 2-48 describes the fields shown in the displays.

**Table 2-48 show ip igmp groups Field Descriptions**

Field	Description
Group Address	Address of the multicast group.
Interface	Interface through which the group is reachable.
Uptime	Time in weeks, days, hours, minutes, and seconds that this multicast group has been known.
Expires	Time in weeks, days, hours, minutes, and seconds until the entry expires. If an entry expires, then the entry (for a short period) shows “now” before it is removed.  “never” indicates that the entry will not time out, because a local receiver is on this router for this entry.  “stopped” indicates that timing out of this entry is not determined by this expire timer. If the router is in INCLUDE mode for a group, then the whole group entry times out after the last source entry has timed out (unless the mode is changed to EXCLUDE mode before it times out).
Last Reporter	Last host to report being a member of the multicast group. Both IGMP v3lite and URD require a v2-report.
Group mode:	Either INCLUDE or EXCLUDE. The group mode is based on the type of membership reports that are received on the interface for the group. In the output for the <b>show ip igmp groups detail</b> command, the EXCLUDE mode also shows the Expires: field for the group entry (not shown in the output).
CSR Grp Exp	Shown for multicast groups in the SSM range. It indicates the time (in hours, minutes, and seconds) since the last received group membership report was received. Cisco IOS software needs to use these reports for the operation of URD and IGMP v3lite, but the reports do not indicate group membership by themselves.
Group source list:	Details of which sources have been requested by the multicast group.
Source Address	IP address of the source.
Uptime	Time since the source state was created.
v3 Exp	Time in hours, minutes, and seconds until the membership for the source times out according to IGMP operations. “stopped” displays if no member uses IGMPv3 (but only IGMP v3lite or URD).
CSR Exp	Time in hours, minutes, and seconds until the membership for the source times out according to IGMP v3lite or URD reports. “stopped” displays if members use only IGMPv3.

*Table 2-48 show ip igmp groups Field Descriptions (continued)*

Field	Description
Fwd	Status of whether the router is forwarding multicast traffic due to this entry.
Flags	Information about the entry. The Remote flag indicates that an IGMPv3 report has been received by this source. The C flag indicates that an IGMP v3lite or URD report was received by this source. The U flag indicates that a URD report was received for this source.

**Related Commands**

Command	Description
<b>ip igmp query-interval</b>	Configures the frequency at which Cisco IOS software sends IGMP host query messages.

# show ip igmp interface

To display the information about the IGMP-interface status and configuration, use the **show ip igmp interface** command.

```
show ip igmp [vrf vrf-name] interface [{interface [interface-number]} | {null interface-number} | {vlan vlan-id}]
```

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
<i>interface</i>	(Optional) Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , <b>atm</b> , and <b>ge-wan</b> .	
<i>interface-number</i>	(Optional) Module and port number; see the “Usage Guidelines” section for valid values.	
<b>null</b> <i>interface-number</i>	Specifies the null interface; the valid value is <b>0</b> .	
<b>vlan</b> <i>vlan-id</i>	Specifies the VLAN; valid values are from 1 to 4094.	

**Defaults** If you do not specify a VLAN, information for VLAN 1 is shown.

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

If you omit the optional arguments, the **show ip igmp interface** command displays information about all interfaces.

**Examples** This example shows how to display IGMP information for VLAN 43:

```
Router# show ip igmp interface vlan 43
Vlan43 is up, line protocol is up
Internet address is 43101014/54
IGMP is enabled on interface
Current IGMP host version is 5
Current IGMP router version is 5
IGMP query interval is 60 seconds
IGMP querier timeout is 450 seconds
```

```

IGMP max query response time is 40 seconds
Last member query count is 5
Last member query response interval is 4000 ms
Inbound IGMP access group is not set
IGMP activity: 4 joins, 0 leaves
Multicast routing is enabled on interface
Multicast TTL threshold is 0
Multicast designated router (DR) is 43101014 (this system)
IGMP querying router is 43101014 (this system)
Multicast groups joined by this system (number of users):
5541014140(4)
IGMP snooping is globally enabled
IGMP snooping is enabled on this interface
IGMP snooping fast-leave is disabled and querier is disabled
IGMP snooping explicit-tracking is enabled on this interface
IGMP snooping last member query interval on this interface is 4000 ms
Router#

```

---

**Related Commands**

Command	Description
<a href="#">clear ip igmp group</a>	Deletes the entries for the IGMP-group cache.
<a href="#">show ip igmp snooping mrouter</a>	Displays the information about the dynamically learned and manually configured multicast router interfaces.

# show ip igmp snooping explicit-tracking

To display the information about the explicit host-tracking status for IGMPv3 hosts, use the **show ip igmp snooping explicit-tracking** command.

```
show ip igmp snooping explicit-tracking {vlan vlan-id}
```

<b>Syntax Description</b>	<b>vlan <i>vlan-id</i></b> Specifies the VLAN; see the “Usage Guidelines” section for valid values.
---------------------------	---

<b>Defaults</b>	If you do not specify a VLAN, information for VLAN 1 is shown.
-----------------	--

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	Explicit host tracking is supported only with IGMPv3 hosts.
-------------------------	---

<b>Examples</b>	This example shows how to display the information about the explicit host-tracking status for IGMPv3 hosts:
-----------------	---

```
Router# show ip igmp snooping explicit-tracking vlan 25
```

```
Source/Group      Interface Reporter Filter_mode
-----
40141414/556151515 V155:4/5 461571513 INCLUDE
40151515/556151515 V155:4/5 461571513 INCLUDE
Router#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">ip igmp snooping explicit-tracking</a>	Enables explicit host tracking.

# show ip igmp snooping mrouter

To display the information about the dynamically learned and manually configured multicast router interfaces, use the **show ip igmp snooping mrouter** command.

```
show ip igmp snooping mrouter [{vlan vlan-id}]
```

<b>Syntax Description</b>	<b>vlan <i>vlan-id</i></b> (Optional) Specifies a VLAN; valid values are from 1 to 4094.
---------------------------	--

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	You can also use the <a href="#">show mac-address-table</a> command to display entries in the MAC-address table for a VLAN that has IGMP snooping enabled.
-------------------------	--

You can display IGMP snooping information for VLAN interfaces by entering the **show ip igmp interface vlan *vlan-num*** command.

<b>Examples</b>	This example shows how to display the information about IGMP snooping for a specific VLAN:
-----------------	--

```
Router# show ip igmp snooping mrouter interface 1
vlan          ports
-----+-----
  4           Gi4/4,Gi5/4,Fa3/48,Router
Router#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">ip igmp snooping mrouter</a>	Configures a Layer 2 port as a multicast router port.

# show ip igmp snooping rate-limit

To display the information about the IGMP snooping rate limit, use the **show ip igmp snooping rate-limit** command.

**show ip igmp snooping rate-limit** [**statistics** | **vlan** *vlan-id*]

Syntax Description	
<b>statistics</b>	(Optional) Displays IGMP snooping statistics.
<b>vlan</b> <i>vlan-id</i>	(Optional) Specifies a VLAN; valid values are from 1 to 4094.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the statistics for IGMP snooping rate limiting:

```
Router# show ip igmp snooping rate-limit statistics
```

```
Max IGMP messages incoming rate : Not configured
Vlan  Incoming rate  Rate-limiting ON  Disable count  Time to Enable
-----+-----+-----+-----+-----+
555   4000           No                0
444   5999           \es              3                485
```

```
Router#
```

This example shows how to display IGMP snooping rate-limit information for a specific VLAN:

```
Router# show ip igmp snooping rate-limit vlan 19
```

```
Max IGMP messages incoming rate : 500 pps
Vlan      Incoming IGMP rate (in pps)
```

```
-----+-----
49       500
```

```
Router#
```

Related Commands	Command	Description
	<a href="#">ip igmp snooping rate</a>	Sets the rate limit for IGMP snooping packets.

# show ip igmp snooping statistics

To display IGMPv3 statistics, use the **show ip igmp snooping statistics** command.

```
show ip igmp snooping statistics [{interface interface [interface-number]} |
  {port-channel number} | {vlan vlan-id}]
```

Syntax Description		
<b>interface</b> <i>interface</i>	(Optional) Displays IGMP statistics for the specified interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , and <b>gigabitethernet</b> .	
<i>interface-number</i>	(Optional) Multicast-related statistics for the specified module and port; see the “Usage Guidelines” section for valid values.	
<b>port-channel</b> <i>number</i>	(Optional) Displays multicast-related statistics for the specified port-channel; valid values are from 1 to 282.	
<b>vlan</b> <i>vlan-id</i>	(Optional) Displays multicast-related statistics for the specified VLAN; valid values for <i>vlan-id</i> are from 1 to 4094.	

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **show ip igmp snooping statistics** command displays the following statistics:

- List of ports that are members of a group
- Filter mode
- Reporter-address behind the port
- Additional information (such as the last-join and last-leave collected since the previous time that a **clear ip igmp snooping statistics** command was issued)

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The **port-channel** *number* values from 257 to 282 are supported on the CSM and the FWSM only.

The #hosts behind the VLAN is displayed only if you define the max-hosts policy on the specified VLAN and enable the log policy for the specified VLAN.

## show ip igmp snooping statistics

### Examples

This example shows how to display IGMPv3 statistics:

```
Router# show ip igmp snooping statistics interface FastEthernet5/1

IGMP Snooping statistics
Service-policy: Policy4policy tied with this interface
#Channels: 3
#hosts : 3
Query Rx: 5904 GS Query Rx: 0 V3 Query Tot Rx: 0
Join Rx: 8686 Leave Rx: 0 V3 Report Rx: 5300
Join Rx from router ports: 8684 Leave Rx from router ports: 0
Total Rx: 44587
Channel/Group      Interface  Reporter  Uptime    Last-Join  Last-Leave
401715014,539141414 F5/4      401515014 00:45:00  4:40:00    -
401713014,539141414 F5/4      401513014 00:50:40  4:40:05    0:30:05
401714014,539141414 F5/4      401514014 00:40:40  4:40:03    -
Router#
```

Table 2-49 describes the fields that are shown in the example.

**Table 2-49 show ip igmp snooping statistics Field Descriptions**

Field	Description
Service-policy: Policy1	Policy tied to this interface.
#Channels: 3	Number of channels behind the specified interface.
#hosts	Number of hosts behind the specified interface. This field is displayed only if max-hosts policy is used.

### Related Commands

Command	Description
<a href="#">clear ip igmp snooping statistics</a>	Clears the IGMP snooping statistics.

# show ip igmp udlr

To display UDLR information for the connected multicast groups on the interfaces that have a UDL helper address configured, use the **show ip igmp udlr** command.

**show ip igmp udlr** [*group-name* | *group-address* | *interface-type interface-number*]

Syntax Description		
	<i>group-name</i>	(Optional) Name of the multicast group.
	<i>group-address</i>	(Optional) Address of the multicast group.
	<i>interface-type interface-number</i>	(Optional) Interface type and number.

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

**Command Modes** User EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command displays which groups are being forwarded and received over the UDL.

On the upstream router, this command shows which interface is a UDL interface and which IP multicast groups are being forwarded out that interface. The UDL Reporter is the IP address of the downstream interface on the receiving router. If there is more than one downstream router, this field shows which downstream router forwarded the IGMP host report to the upstream router over the ground-based network. This report is forwarded over the UDL so that all downstream routers know which groups have already been requested by other downstream routers, and additional IGMP host reports are suppressed.

On the downstream router, this command (in the Interface field) shows which local interface received an IGMP host report (from a connected host for a specific group). The UDL Reporter is the IP address of the router that had forwarded the IGMP host report to the upstream router over the ground-based network. The UDL Interfaces column shows the interface on which IP multicast packets are being received.

**Examples** This example shows the output of the **show ip igmp udlr** command on an upstream router:

```
Router# show ip igmp udlr

IGMP UDLR Status, UDL Interfaces: Serial0
Group Address      Interface      UDL Reporter    Reporter Expires
5541514571554     Serial0       40101015        00:05:45
5541014140        Serial0       40101015        00:05:44
555171717         Serial0       40101015        00:05:45
Router#
```

This example shows the output of the **show ip igmp udldr** command on a downstream router:

```
Router# show ip igmp udldr

IGMP UDLR Status, UDL Interfaces: Serial0
Group Address   Interface      UDL Reporter   Reporter Expires
5541514571554  Serial0       40101015       00:05:49
5541014140     Serial0       40101015       00:05:48
555171717      Serial0       40101015       00:05:55
Router#
```

[Table 2-50](#) describes the fields shown in the output of the **show ip igmp udldr** command.

**Table 2-50** *show ip igmp udldr Field Descriptions*

Field	Description
Group Address	All group's helper addresses on the interface.
Interface	Interface type and number to which the group is connected.
UDL Reporter	IP address of the router on the UDL network that is IGMP helping for the group.
Reporter Expires	How soon the UDL Reporter will become inactive, in hours:minutes:seconds. This can occur under the following conditions: <ul style="list-style-type: none"> <li>• The UDL Reporter has become nonoperational.</li> <li>• The link or network to the reporter has become nonoperational.</li> <li>• The group member attached to the UDL Reporter has left the group.</li> </ul>

# 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	<i>type</i>	(Optional) Interface type.
	<i>number</i>	(Optional) Interface number.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The Cisco IOS software automatically enters a directly connected route in the routing table if the interface is usable. A usable interface is one through which the software can send and receive packets. If the software determines that an interface is not usable, it removes the directly connected routing entry from the routing table. Removing the entry allows the software to use dynamic routing protocols to determine backup routes to the network, if any.

If the interface can provide two-way communication, the line protocol is marked “up.” If the interface hardware is usable, the interface is marked “up.”

If you specify an optional interface type, you see only information on that specific interface.

If you specify no optional arguments, you see information on all the interfaces.

When an asynchronous interface is encapsulated with PPP or Serial Line Internet Protocol (SLIP), IP fast switching is enabled. The **show ip interface** command on an asynchronous interface that is encapsulated with PPP or SLIP displays a message indicating that IP fast switching is enabled.

**Examples** This example shows how to display the usability status for a specific VLAN:

```
Router# show ip interface vlan 1
Vlan4 is up, line protocol is up
  Internet address is 401615814/54
  Broadcast address is 555155515551555
  Address determined by non-volatile memory
  MTU is 4500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
```

## ■ show ip interface

```

Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable 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
Router#

```

Table 2-51 describes the fields that are shown in the example.

**Table 2-51** show ip interface Field Descriptions

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 2-51** *show ip interface Field Descriptions (continued)*

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 the split horizon.
ICMP redirects	Status of the redirect messages on this interface.
ICMP unreachable	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.

# show ip mcache

To display the contents of the IP fast-switching cache, use the **show ip mcache** command.

```
show ip mcache [vrf vrf-name] [group-address | group-name] [source-address | source-name]
```

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
<i>group-address</i> / <i>group-name</i>	(Optional) Fast-switching cache for the single group.	
<i>source-address</i> / <i>source-name</i>	(Optional) If the source address or name is also specified, displays a single multicast cache entry.	

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The *group-address* / *group-name* can be either a Class D IP address or a DNS name.  
The *source-address* / *source-name* can be either a unicast IP address or a DNS name.

**Examples** This example shows how to display the contents of the IP fast-switching cache. This entry shows a specific source (wrn-source 226.62.246.73) sending to the World Radio Network group (224.2.143.24):

```
Router> show ip mcache wrn wrn-source
```

```
IP Multicast Fast-Switching Cache
(5561651546173/35, 554151443154), Fddi0, Last used: 00:00:00
 Ethernet0      MAC Header: 04005E058F480000C4883D30800
 Ethernet4      MAC Header: 04005E058F480000C4883D60800
 Ethernet5      MAC Header: 04005E058F480000C4883D40800
 Ethernet3      MAC Header: 04005E058F480000C4883D70800
```

[Table 2-52](#) describes the fields shown in the display.

**Table 2-52 show ip mcache Field Descriptions**

Field	Description
226.62.246.73	Source address.
224.2.143.24	Destination address.
Fddi0	Incoming or expected interface on which the packet should be received.

*Table 2-52 show ip mcache Field Descriptions (continued)*

Field	Description
Last used:	Latest time that the entry was accessed for a packet that was successfully fast switched. “Semi-fast” indicates that the first part of the outgoing interface list is fast switched and the rest of the list is process level switched.
Ethernet0 MAC Header:	Outgoing interface list and respective MAC header that is used when rewriting the packet for output. If the interface is a tunnel, the MAC header shows the real next-hop MAC header and, in parentheses, the real interface name.

# show ip mds interface

To display MDS information for all the interfaces on the module, use the **show ip mds interface** command.

**show ip mds interface** [*vrf vrf-name*]

Syntax Description	<b>vrf vrf-name</b>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
--------------------	---------------------	--

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display MDS information for all the interfaces on the module:

```
Router# show ip mds interface
```

Interface	SW-Index	HW-Index	HW IDB	FS Vector	VRF
Ethernet4/0/0	5	4	0x60C5DB40	0x605FB7A4	default
Ethernet4/0/4	3	5	0x60C35580	0x603D55B8	default
Ethernet4/0/5	4	3	0x60C35E40	0x605FB7A4	default
Ethernet4/0/3	5	4	0x60C39E60	0x603D55B8	default
Ethernet4/0/4	6	5	0x60C3D780	0x605FB7A4	default
Ethernet4/0/5	7	6	0x60C44440	0x605FB7A4	default
Ethernet4/0/6	8	7	0x60C453A0	0x605FB7A4	default
Ethernet4/0/7	9	8	0x60C48DC0	0x605FB7A4	default
POS5/0/0	40	9	0x0		default
POS3/0/0	44	40	0x0		default
Virtual-Access4	43	44	0x0		default
Loopback0	44	45	0x0		default
Tunnel0	45	53	0x64C5E480	0x603D55B8	vrf4
Tunnel4	46	54	0x64C567E0	0x603D55B8	vrf5
Ethernet4/0/314	47	4	0x60C39E60	0x603D55B8	vrf4
Ethernet4/0/315	48	4	0x60C39E60	0x603D55B8	vrf5

Table 2-53 describes the fields shown in the display.

**Table 2-53** show ip mds interface Field Descriptions

Field	Description
Interface	Specified interface.
SW-Index	Software index.
HW-Index	Hardware index.
HW IDB	Hardware interface description block.
VRF	VPN routing/forwarding instance.

# show ip mpacket

To display the contents of the circular cache-header buffer, use the **show ip mpacket** command.

```
show ip mpacket [vrf vrf-name] [group-address | group-name] [source-address | source-name]
[detail]
```

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
<i>group-address</i>   <i>group-name</i>	(Optional) Cache headers matching the specified group address or group name.	
<i>source-address</i>   <i>source-name</i>	(Optional) Cache headers matching the specified source address or source name.	
<b>detail</b>	(Optional) In addition to the summary information, displays the rest of the IP header fields on an additional line, plus the first 8 bytes after the IP header (usually the UDP port numbers).	

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command is applicable only when the **ip multicast cache-headers** command is in effect. Each time that this command is entered, a new buffer is allocated. The summary display (when the **detail** keyword is omitted) shows the IP packet identifier, time-to-live (TTL) value, source and destination IP addresses, and a local time stamp when the packet was received. The two arguments and one keyword can be used in the same command in any combination.

**Examples** This example shows how to display the contents of the circular cache-header buffer:

```
Router # show ip mpacket smallgroup

IP Multicast Header Cache - entry count:6, next index: 7
Key: id/ttl timestamp (name) source group

D785/447 5064461908 (ABC-xylcompany1com) 49514681558140 554151617
7305/443 5064471908 (school1edu) 44714515147 554151617
6CB5/444 5064471445 (MSSRS1company1com) 45415149140 554151617
D785/447 5064471868 (ABC-xylcompany1com) 49514681558140 554151617
E5E9/453 5064481488 (Newman1com) 5441418140 554151617
4CA7/457 5064481544 (teller1company1com) 495146816140 554151617
```

Table 2-54 describes the fields shown in the display.

**Table 2-54** *show ip mpacket Field Descriptions*

Field	Description
entry count	Number of packets cached (one packet for each line in the display). The cache has lines numbered from 0 to 1024.
next index	Index for the next element in the cache.
id	Identification number of the IP packet.
ttl	Current TTL of the packet.
timestamp	Time-stamp sequence number of the packet.
(name)	DNS name of the source sending to the group. Name appears in parentheses.
source	IP address of the source sending to the group.
group	Multicast group address to which the packet is sent. In this example, the group address is the group name smallgroup.

#### Related Commands

Command	Description
<a href="#">ip multicast cache-headers</a>	Allocates a circular buffer to store IP multicast packet headers that the router receives.

# show ip mroute

To display the information about the IP-multicast routing table, use the **show ip mroute** command.

```
show ip mroute [vrf vrf-name] [{interface interface-number} | {null interface-number} |
  {port-channel number} | {vlan vlan-id} | {{host-name / host-address} [source]}] | {active
  [kbps | {interface-type num}] } | {count | pruned | static | summary }
```

Syntax	Description
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
<i>interface</i>	(Optional) Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , <b>atm</b> , and <b>ge-wan</b> .
<i>interface-number</i>	(Optional) Module and port number; see the “Usage Guidelines” section for valid values.
<b>null</b> <i>interface-number</i>	(Optional) Specifies the null interface; the valid value is <b>0</b> .
<b>port-channel</b> <i>number</i>	(Optional) Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 282.
<b>vlan</b> <i>vlan-id</i>	(Optional) Specifies the VLAN; valid values are from 1 to 4094.
<i>host-name</i>   <i>host-address</i>	(Optional) Name or IP address as defined in the DNS hosts table.
<i>source</i>	(Optional) IP address or name of a multicast source.
<b>active</b>	(Optional) Displays the rate that active sources are sending to multicast groups.
<i>kbps</i>	(Optional) Minimum rate at which active sources are sending to multicast groups; active sources sending at this rate or greater are displayed. Valid values are from 1 to 4294967295 kbps.
<b>count</b>	(Optional) Displays the route and packet count information.
<b>pruned</b>	(Optional) Displays the pruned routes.
<b>static</b>	(Optional) Displays the static multicast routes.
<b>summary</b>	(Optional) Displays a one-line, abbreviated summary of each entry in the IP-multicast routing table.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

If you omit all optional arguments and keywords, the **show ip mroute** command displays all entries in the IP-multicast routing table.

The **show ip mroute active kbps** command displays all sources sending at a rate greater than or equal to *kbps*.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The **port-channel number** values are from 257 to 282 are supported on the CSM and the FWSM only.

The multicast routing table is populated by creating source, group (S,G) entries from star, group (\*,G) entries. The star refers to all source addresses, the “S” refers to a single source address, and the “G” is the destination multicast group address. In creating (S,G) entries, the software uses the best path to that destination group that is found in the unicast routing table (through RPF).

**Examples**

This example shows how to display all entries in the IP-multicast routing table:

```
Router# show ip mroute 224.1.1.1
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, 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 - Candidate MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, ] - Multicast Tunnel
       \ - Joined MDT-data group, y - Sending to MDT-data group, s - SSM
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 554141414), 00:00:07/00:05:59, RP 5101014, flags: BC
  Bidir-Upstream: Null, RPF nbr 0101010, RPF-MFD
  Outgoing interface list:
    Vlan505, Forward/Sparse-Dense, 00:00:07/00:05:59, H
Router#
```

This example shows how to display the rate that active sources are sending to multicast groups and to display only active sources sending at greater than the default rate:

```
Router# show ip mroute active

Active IP Multicast Sources - sending >= 4 kbps

Group: 5541514571554, (sdr1cisco1com)
  Source: 4461437158169 (mbonelipd1an11gov)
  Rate: 4 pps/4 kbps(4sec), 4 kbps(last 4 secs), 4 kbps(life avg)

Group: 5541515041544, ACM 97
  Source: 43014591551460 (webcast3-e41acm971interoplnet)
  Rate: 9 pps/93 kbps(4sec), 445 kbps(last 50 secs), 85 kbps(life avg)

Group: 5541515071545, ACM 97
  Source: 43014591551460 (webcast3-e41acm971interoplnet)
  Rate: 3 pps/34 kbps(4sec), 63 kbps(last 49 secs), 65 kbps(life avg)
Router#
```

This example shows how to display the information about the route and packet count:

```
Router# show ip mroute count
IP Multicast Statistics
56 routes using 58555 bytes of memory
43 groups, 3130 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:554151436189, Source count:4, Group pkt count:59054
Source:4351506175158/35, Forwarding:59054/-578/4486/0, Other:85754/8/56665
Router#
```

This example shows how to display summary information:

```
Router# 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

Router#
```

Table 2-55 describes the fields that are shown in the example.

**Table 2-55** *show ip mroute Field Descriptions*

Field	Description
Flags:	Information about the entry.
D - Dense	Entry is operating in dense mode.
S - Sparse	Entry is operating in sparse mode.
s - SSM Group	Entry is a member of an SSM group.
C - Connected	Member of the multicast group is present on the directly connected interface.
L - Local	Router 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 whether the (S,G) entry is pointing toward the route processor. This field shows a prune state along the shared tree for a particular source.
F - Register flag	Status of whether the software is registering for a multicast source.
T - SPT-bit set	Status of whether the packets have been received on the shortest-path tree.

Table 2-55 show ip mroute Field Descriptions (continued)

Field	Description
J - Join SPT	<p>For (*, G) entries, indicates that the rate of traffic flowing down the shared tree is exceeding the SPT-Threshold that is 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 that is received down the shared tree triggers an (S,G) join in the direction of the source causing the router to join the source tree.</p> <p>For (S,G) entries, indicates that the entry was created because the SPT-Threshold for the group was exceeded. When the J - Join SPT flag is set for (S,G) entries, the router 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 1 minute.</p> <p>The router measures the traffic rate on the shared tree and compares the measured rate to the group's SPT-Threshold once every second. If the traffic rate exceeds the SPT-Threshold, the J - Join SPT flag is set on the (*, G) entry until the next measurement of the traffic rate. The flag is cleared when the next packet arrives on the shared tree and a new measurement interval is started.</p> <p>If the default SPT-Threshold value of 0 Kbps is used for the group, the J - Join SPT flag is always set on (*, G) entries and is never cleared. When the default SPT-Threshold value is used, the router immediately switches to the shortest-path tree when traffic from a new source is received.</p>
Bidir-Upstream: Null, RPF nbr 0.0.0.0, RPF-MFD	Interface that is used to reach the PIM route processor. Set to Null if the router is the PIM route processor or if no route exists to the PIM route processor.
Outgoing interface flags:	Information about the outgoing entry.
H - Hardware switched	Entry is hardware switched.
Timers:	Uptime/Expires.
Interface state:	Interface, Next-Hop or VCD, State/Mode.
(*, 224.0.255.1) (198.92.37.100/32, 224.0.255.1)	<p>Entry in the IP-multicast routing table. The entry consists of the IP address of the source router followed by the IP address of the multicast group. An asterisk (*) in place of the source router indicates all sources.</p> <p>Entries in the first format are referred to as (*,G) or "star comma G" entries. Entries in the second format are referred to as (S,G) or "S comma G" entries. (*,G) entries are used to build (S,G) entries.</p>
uptime	Hours, minutes, and seconds that the entry has been in the IP-multicast routing table.
expires	Hours, minutes, and seconds until the entry is removed from the IP-multicast routing table on the outgoing interface.

Table 2-55 show ip mroute Field Descriptions (continued)

Field	Description
RP	Address of the route processor. For routers 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 router to the source. Tunneling indicates that this router is sending data that is encapsulated in register packets to the route processor. The hexadecimal number in parentheses indicates to which route processor it is registering. Each bit indicates a different route processor if multiple route processors per group are used.
Dvmrp or Mroute	Status of whether the RPF information is obtained from the DVMRP routing table or the static mroute configuration.
Outgoing interface list:	Interfaces through which packets are forwarded. When you enable the <b>ip pim nbma-mode</b> command 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 the 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 whether the packets are forwarded on the interface if there are no restrictions due to access lists or the TTL threshold. Following the slash (/), the 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, the duration in hours, minutes, and seconds that the entry has been in the IP-multicast routing table. Specifies that following the slash (/), the duration in hours, minutes, and seconds until the entry is removed from the IP-multicast routing table.

## Related Commands

Command	Description
<b>ip multicast-routing</b>	Enables IP multicast routing.
<b>ip pim</b>	Enables PIM on an interface.

# show ip mroute bidirectional

To display Bidir information from the IP-multicast routing table, use the **show ip mroute bidirectional** command.

```
show ip mroute bidirectional [{interface interface-number} | {null interface-number} |
  {port-channel number} | {vlan vlan-id} | {{host-name / host-address} [source]} | {active
  [kbps | {interface-type num}]} | {count | pruned | static | summary}]
```

Syntax Description	
<i>interface</i>	(Optional) Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , <b>atm</b> , and <b>ge-wan</b> .
<i>interface-number</i>	Module and port number; see the “Usage Guidelines” section for valid values.
<b>null</b> <i>interface-number</i>	Specifies the null interface; the valid value is <b>0</b> .
<b>port-channel</b> <i>number</i>	Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 282.
<b>vlan</b> <i>vlan-id</i>	Specifies the VLAN; valid values are from 1 to 4094.
<i>host-name</i>   <i>host-address</i>	(Optional) Name or IP address as defined in the DNS hosts table.
<i>source</i>	(Optional) IP address or name of a multicast source.
<b>active</b>	(Optional) Displays the rate that active sources are sending to multicast groups.
<i>kbps</i>	(Optional) Minimum rate at which active sources are sending to multicast groups; active sources sending at this rate or greater are displayed. Valid values are from 1 to 4294967295 kbps.
<b>count</b>	(Optional) Displays the route and packet count.
<b>pruned</b>	(Optional) Displays the pruned routes.
<b>static</b>	(Optional) Displays the static multicast routes.
<b>summary</b>	(Optional) Displays a one-line, abbreviated summary of each entry in the IP-multicast routing table.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---

**Usage Guidelines**

If you omit all optional arguments and keywords, the **mroute bidirectional** command displays all entries in the IP-multicast routing table.

---

**Examples**

This example shows how to display the information in the IP-multicast routing table that is related to bidirectional PIM:

```
Router# show ip mroute bidirectional
(*, 555141310), 00:00:05/00:05:57, RP 3131313, flags:BC
Bidir-Upstream:GigabitEthernet5/4, RPF nbr 401531417, RPF-MFD
Outgoing interface list:
GigabitEthernet5/4, Bidir-Upstream/Sparse-Dense, 00:00:05/00:00:00,H
Vlan30, Forward/Sparse-Dense, 00:00:05/00:05:57, H
(*, 555141510), 00:00:04/00:05:55, RP 3131313, flags:BC
Bidir-Upstream:GigabitEthernet5/4, RPF nbr 401531417, RPF-MFD
Outgoing interface list:
GigabitEthernet5/4, Bidir-Upstream/Sparse-Dense, 00:00:04/00:00:00,H
Vlan30, Forward/Sparse-Dense, 00:00:04/00:05:55, H
(*, 555141414), 00:00:00/00:05:59, RP 3131313, flags:BC
Bidir-Upstream:GigabitEthernet5/4, RPF nbr 401531417, RPF-MFD
Outgoing interface list:
GigabitEthernet5/4, Bidir-Upstream/Sparse-Dense, 00:00:00/00:00:00,H
Vlan30, Forward/Sparse-Dense, 00:00:00/00:05:59, H
Router#
```

## show ip msdp count

To display the number of sources and groups that originated in MSDP source-active messages and the number of source-active messages from an MSDP peer in the source-active cache, use the **show ip msdp count** command.

```
show ip msdp [vrf vrf-name] count [as-number]
```

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
<i>as-number</i>	(Optional) Number of sources and groups that originated in source-active messages from the specified autonomous system number.	

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** You must enter the **ip msdp cache-sa-state** command for this command to obtain any output from the **show ip msdp** command.

**Examples** This example shows how to display the number of sources and groups that originated in MSDP source-active messages and the number of source-active messages from an MSDP peer in the source-active cache:

```
Router# show ip msdp count

SA State per Peer Counters, <Peer>: <# SA learned>
554143515501446: 54
47514615401553: 3964
4751461553149: 40
47514614701440: 44

SA State per ASN Counters, <asn>: <# sources>/<# groups>
Total entries: 4009
?: 495/98, 9: 4/4, 44: 407/57, 47: 7/5
48: 4/3, 55: 53/47, 56: 39/57, 57: 5/5
35: 49/7, 38: 5/4, 55: 4/4, 57: 4/4
68: 4/4, 73: 45/8, 84: 49/4, 87: 9/6
1
1
1
```

Table 2-56 describes the fields shown in the display.

**Table 2-56** *show ip msdp count* Field Descriptions

Field	Description
224.135.250.116: 24	MSDP peer with IP address 224.135.250.116: 24 source-active messages from the MSDP peer in the source-active cache.
Total entries	Total number of source-active entries in the source-active cache.
9: 1/1	Autonomous system 9: 1 source/1 group.

#### Related Commands

Command	Description
<a href="#">ip msdp cache-sa-state</a>	Creates a source-active state on the router.

## show ip msdp peer

To display detailed information about the MSDP peer, use the **show ip msdp peer** command.

```
show ip msdp [vrf vrf-name] peer [peer-address | peer-name]
```

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
<i>peer-address</i>   <i>peer-name</i>	(Optional) DNS name or IP address of the MSDP peer for which information is displayed.	

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display detailed information about the MSDP peer:

```
Router# show ip msdp peer 224.135.250.116

MSDP Peer 554143515501446 (rtp5-rp41cisco1com), AS 409 (configured AS)
Description:
Connection status:
  State: Up, Resets: 9, Connection source: Loopback5 (5581691499147)
  Uptime(Downtime): 4d40h, Messages sent/received: 436765/459065
  Output messages discarded: 0
  Connection and counters cleared 4w5d ago
SA Filtering:
  Input (S,G) filter: none, route-map: none
  Input RP filter: none, route-map: none
  Output (S,G) filter: none, route-map: none
  Output RP filter: none, route-map: none
SA-Requests:
  Input filter: none
  Sending SA-Requests to peer: disabled
Peer ttl threshold: 0
SAs learned from this peer: 35, SAs limit: 500
Input queue size: 0, Output queue size: 0
```

[Table 2-57](#) describes the fields shown in the display.

**Table 2-57** show ip msdp peer Field Descriptions

Field	Description
MSDP Peer	IP address of the MSDP peer.
AS	Autonomous system to which the MSDP peer belongs.
State:	State of the MSDP peer.
Connection source:	Interface used to obtain the IP address for the TCP local connection address.
Uptime(Downtime):	Days and hours that the MSDP peer is up or down. If the time is less than 24 hours, it is shown in hours:minutes:seconds.
Messages sent/received:	Number of source-active messages sent to the MSDP peer/number of source-active messages received from the MSDP peer.
SA Filtering:	Information regarding access list filtering of source-active input and output if any.
SA-Requests:	Information regarding access list filtering of source-active requests if any.
SAs learned from this peer:	Number of source-active messages from the MSDP peer in the source-active cache.
SAs limit:	Source-active message limit for this MSDP peer.

**Related Commands**

Command	Description
<a href="#">ip msdp peer</a>	Configures an MSDP peer.

# show ip msdp sa-cache

To display the (S,G) state that is learned from MSDP peers, use the **show ip msdp sa-cache** command.

```
show ip msdp [vrf vrf-name] sa-cache [group-address | source-address | group-name |
source-name] [group-address | source-address | group-name | source-name] [as-number]
```

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
<i>group-address</i>   <i>source-address</i>   <i>group-name</i>   <i>source-name</i>	(Optional) Group address, source address, group name, or source name of the group or source about which (S,G) information is displayed.	
<i>as-number</i>	(Optional) Only state originated by the autonomous system number specified is displayed.	

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The state is cached only if you enter the **ip msdp cache-sa-state** command. If you specify two addresses or names, an (S,G) entry corresponding to those addresses is displayed. If you specify one group address only, all sources for that group are displayed. If no options are specified, the entire source-active cache is displayed.

**Examples** This example shows how to display the (S,G) state that is learned from MSDP peers:

```
Router# show ip msdp sa-cache

MSDP Source-Active Cache - 5398 entries
(475146144133, 5381405144810), RP 475146131444, MBGP/AS 704, 5d40h/00:05:33
(475146144518, 554151014), RP 49514681500165, MBGP/AS 40888, 00:03:54/00:05:38
(475146140143, 55713713514), RP 495146813195, MBGP/AS 704, 05:55:50/00:03:35
(475146166148, 533101014), RP 4951468131444, MBGP/AS 704, 5d40h/00:05:35
(4751461661448, 533101014), RP 4951468131444, MBGP/AS 704, 5d40h/00:05:35
(475146140143, 55713713515), RP 495146813195, MBGP/AS 704, 00:44:30/00:04:34
(4751461701503, 55415153615), RP 4951468155317, MBGP/AS 3585, 05:34:46/00:05:49
(4751481451404, 536149515615), RP 495146813195, MBGP/AS 704, 04:54:43/00:05:55
(475146140143, 55713713513), RP 495146813195, MBGP/AS 704, 00:44:30/00:05:34
(475148145143, 5541019513), RP 49514681500165, MBGP/AS 40888, 6d09h/00:05:35
(4751481451444, 5541019513), RP 49514681500165, MBGP/AS 40888, 46:48:08/00:05:35
(475148154145, 5541019513), RP 49514681500165, MBGP/AS 40888, 46:48:08/00:05:35
(475148145175, 5541019513), RP 49514681500165, MBGP/AS 40888, 08:40:55/00:05:35
```

```
(4751481451400, 5541019513), RP 49514681500165, MBGP/AS 40888, 08:40:55/00:05:35
(475146140143, 55713713516), RP 495146813195, MBGP/AS 704, 00:45:30/00:05:34
(475148144133, 55415471558140), RP 4951468131444, MBGP/AS 704, 5d40h/00:05:35
(47514815551540, 554151554143), RP 495146813195, MBGP/AS 704, 04:54:53/00:05:55
(475148144133, 55915341454143), RP 4951468131444, MBGP/AS 704, 5d40h/00:05:33
(4751481351438, 554151500153), RP 4951468155317, MBGP/AS 3585, 54:33:40/00:05:49
(4751481751544, 554151500153), RP 4951468155317, MBGP/AS 3585, 54:33:40/00:05:49
```

Table 2-58 describes the fields shown in the display.

**Table 2-58** show ip msdp sa-cache Field Descriptions

Field	Description
(172.16.41.33, 238.105.148.0)	First address (source) that is sending to the second address (group).
RP 172.16.3.111	Rendezvous point address in the originating domain where the source-active messages started.
MBGP/AS 704	Rendezvous point that is in autonomous system 704 according to multiprotocol BGP.
2d10h/00:05:33	Route that has been cached for 2 days and 10 hours. If no source-active message is received in 5 minutes and 33 seconds, the route is removed from the source-active cache.

#### Related Commands

Command	Description
<b>clear ip msdp sa-cache</b>	Clears MSDP source active cache entries.
<b>ip msdp cache-sa-state</b>	Creates a source-active state on the router.

# show ip msdp summary

To display the MSDP peer status, use the **show ip msdp summary** command.

**show ip msdp** [*vrf vrf-name*] **summary**

<b>Syntax Description</b>	<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
---------------------------	----------------------------	--

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

**Command Modes** EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the MSDP peer status:

```
Router# show ip msdp summary
```

```
MSDP Peer Status Summary
Peer Address      AS      State    Uptime/  Reset SA   Peer Name
                  AS              Downtime Count Count
554143515501446  409     Up       4d40h    9       444    rtp5-rp4
*47515015401553  4539    Up       44:54:00 5       4040   sl-rp-stk
4751461553149    409     Up       45:36:47 5       40     shinjuku-rp4
47514614701440   409     Up       4d44h    9       45     ams-rp4
```

Table 2-59 describes the fields shown in the display.

**Table 2-59 show ip msdp summary Field Descriptions**

<b>Field</b>	<b>Description</b>
Peer Address	IP address of the MSDP peer.
AS	Autonomous system to which the MSDP peer belongs.
State	State of the MSDP peer.
Uptime/Downtime	Days and hours that the MSDP peer is up or down per the state that is shown in the previous column. If the time is less than 24 hours, it is shown in hours:minutes:seconds.
SA Count	Number of source-active messages from this MSDP peer in the source-active cache.
Peer Name	Name of the MSDP peer.

# show ip nhrp

To display information about the NHRP cache, use the **show ip nhrp** command.

```
show ip nhrp [summary | dynamic | static | incomplete] [{interface-type interface-number} |
ip-address] [detail | brief]
```

Syntax Description		
<b>summary</b>	(Optional)	Displays a summary of NHRP cache purge information.
<b>dynamic</b>	(Optional)	Displays the dynamic (learned) IP-to-NBMA cache entries only.
<b>static</b>	(Optional)	Displays the static IP-to-NBMA address cache entries only (configured using the <b>ip nhrp map</b> command).
<b>incomplete</b>	(Optional)	Displays information about an incomplete cache.
<i>interface-type</i> <i>interface-number</i>	(Optional)	NHRP cache information for the specified interface type only; see <a href="#">Table 2-60</a> for types, number ranges, and descriptions.
<i>ip-address</i>	(Optional)	NHRP cache information for the specified IP address only.
<b>detail</b>	(Optional)	Displays detailed information about the NHRP cache.
<b>brief</b>	(Optional)	Displays basic information about the NHRP cache.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** [Table 2-60](#) lists the valid types, number ranges, and descriptions for the *type* and *number* optional arguments.



**Note** The valid types can vary according to the platform and interfaces on the platform.

**Table 2-60 Valid Types, Number Ranges, and Interface Descriptions**

Valid Types	Number Ranges	Interface Descriptions
<b>async</b>	1	Async
<b>ctunnel</b>	0 to 2147483647	C-Tunnel
<b>dialer</b>	0 to 20049	Dialer
<b>fastethernet</b>	0 to 6	Fast Ethernet IEEE 802.3
<b>GigabitEthernet</b>	0 to 6	Gigabit Ethernet IEEE 802.3

**Table 2-60 Valid Types, Number Ranges, and Interface Descriptions (continued)**

Valid Types	Number Ranges	Interface Descriptions
<b>loopback</b>	0 to 2147483647	Loopback
<b>mfr</b>	0 to 2147483647	Multilink Frame Relay bundle
<b>multilink</b>	0 to 2147483647	Multilink-group
<b>null</b>	0	Null
<b>port-channel</b>	1 to 282	EtherChannel of interfaces
<b>pos-channel</b>	1 to 4094	PoS channel of interfaces
<b>tunnel</b>	0 to 2147483647	Tunnel interfaces
<b>vif</b>	1	PGM multicast host
<b>tunnel</b>	0 to 2147483647	Tunnel
<b>virtual-template</b>	1 to 1000	Virtual template
<b>virtual-tokenring</b>	0 to 2147483647	Virtual Token Ring
<b>xtagatm</b>	0 to 2147483647	Extended tag ATM

**Examples**

This example shows how to display information about the NHRP cache:

```
Router# show ip nhrp

40101015 555155515551555, ATM0/0 created 0:00:43 expire 4:59:46
  Type: dynamic Flags: authoritative
  NBMA address: 4414444144441444414444144441444414444144441444414444144
40101014 555155515551555, Tunnel0 created 0:40:03 expire 4:49:56
  Type: static Flags: authoritative
  NBMA address: 44141415
```

Table 2-61 describes the fields shown in the display.

**Table 2-61 show ip nhrp Field Descriptions**

Field	Description
10.0.0.2 255.255.255.255	IP address and its network mask in the IP-to-NBMA address cache. The mask is currently always 255.255.255.255 because aggregation of NBMA information through NHRP is not supported.
ATM0/0 created 0:00:43	Interface type and number (in this case, ATM slot and port numbers) and when it was created (hours:minutes:seconds).
expire 1:59:16	Time in which the positive and negative authoritative NBMA address will expire (hours:minutes:seconds). This value is based on the <b>ip nhrp holdtime</b> command.
Type	<ul style="list-style-type: none"> <li>dynamic—NBMA address was obtained from the NHRP Request packet.</li> <li>static—NBMA address was statically configured.</li> </ul>

Table 2-61 show ip nhrp Field Descriptions (continued)

Field	Description
Flags	<ul style="list-style-type: none"> <li>• authoritative—Indicates that the NHRP information was obtained from the next-hop server or router that maintains the NBMA-to-IP address mapping for a particular destination.</li> <li>• implicit—Indicates that the information was learned not from an NHRP request generated from the local router, but from an NHRP packet being forwarded or from an NHRP request being received by the local router.</li> <li>• negative—For negative caching; indicates that the requested NBMA mapping could not be obtained.</li> </ul>
NBMA address	Nonbroadcast multiaccess address. The address format is appropriate for the type of network being used (for example, ATM, Ethernet, SMDS, or multipoint tunnel).

This example shows how to display basic information about the dynamic (learned) IP-to-NBMA cache entries only for a specific IP address:

```
Router# show ip nhrp dynamic 255.255.255.255 brief
      Target      Via          NBMA          Mode      Intfc      Claimed
```

#### Related Commands

Command	Description
<b>ip nhrp holdtime</b>	Changes the number of seconds that NHRP NBMA addresses are advertised as valid in authoritative NHRP responses.
<b>ip nhrp map</b>	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an MBMA network.

# show ip pim bsr-router

To display the BSR information, use the **show ip pim bsr-router** command.

**show ip pim vrf *vrf-name* bsr-router**

<b>Syntax Description</b>	<b>vrf <i>vrf-name</i></b>	Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
---------------------------	----------------------------	---

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

**Command Modes** EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The output includes elected BSR information and information about the locally configured candidate rendezvous-point advertisement.

**Examples** This example shows how to display the BSR information:

```
Router# show ip pim bsr-router

PIMv5 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 4751461443158
  Uptime: 04:37:59, BSR Priority: 4, Hash mask length: 30
  Next bootstrap message in 00:00:03 seconds

Next Cand_RP_advertisement in 00:00:03 seconds1
  RP: 4751461443158(Ethernet0), Group acl: 6
```

[Table 2-62](#) describes the fields shown in the display.

**Table 2-62 show ip pim bsr Field Descriptions**

<b>Field</b>	<b>Description</b>
BSR address	IP address of the bootstrap router.
Uptime	Length of time that this router has been up, in hours, minutes, and seconds.
BSR Priority	Priority as configured in the <b>ip pim bsr-candidate</b> command.
Hash mask length	Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called. This value is configured in the <b>ip pim bsr-candidate</b> command.

*Table 2-62 show ip pim bsr Field Descriptions (continued)*

Field	Description
Next bootstrap message in	Time in hours, minutes, and seconds in which the next bootstrap message is due from this BSR.
Next Cand_RP_advertisement in	Time in hours, minutes, and seconds in which the next candidate rendezvous-point advertisement will be sent.
RP	List of IP addresses of rendezvous points.
Group acl	Standard IP access list number that defines the group prefixes that are advertised in association with the rendezvous-point address. This value is configured in the <b>ip pim bsr-candidate</b> command.

**Related Commands**

Command	Description
<b>ip pim bsr-candidate</b>	Configures the router to announce its candidacy as a BSR.
<b>ip pim rp-candidate</b>	Configures the router to advertise itself as a PIM Version 2 rendezvous-point candidate to the BSR.
<b>show ip pim rp-hash</b>	Displays which rendezvous point is being selected for a specified group.

## show ip pim interface df

To display information about the designated forwarder interface, use the **show ip pim interface df** command.

```
show ip pim vrf vrf-name interface df [rp-addr]
```

### Syntax Description

<b>vrf</b> <i>vrf-name</i>	Specifies the name that is assigned to the multicast VRF instance.
<i>rp-addr</i>	(Optional) Hostname or IP address of the designated forwarder.

### Defaults

If you do not specify *rp-addr*, all designated forwarders are displayed.

### Command Modes

EXEC

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Examples

This example shows how to display the information about the DF interface:

```
Router# show ip pim interface df 10.18.1.31
Interface          RP           DF Winner      Metric      Uptime
Vlan70             4014814134   4017014155     0           44:46:54
FastEthernet5/5    4014814134   4014614130     0           44:46:54
FastEthernet5/6    4014814134   4014814134     0           44:46:54
Router#
```

# show ip pim mdt bgp

To display the detailed BGP advertisement of the route distinguisher for the MDT default group, use the **show ip pim mdt bgp** command.

**show ip pim vrf *vrf-name* mdt bgp**

<b>Syntax Description</b>	<b>vrf <i>vrf-name</i></b> Specifies the name that is assigned to the multicast VRF instance.				
<b>Defaults</b>	This command has no default settings.				
<b>Command Modes</b>	EXEC				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(18)ZY</td> <td>Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)ZY	Support for this command was introduced.
Release	Modification				
12.2(18)ZY	Support for this command was introduced.				

## Examples

This example shows how to display the detailed BGP advertisement of the route distinguisher for the MDT default group:

```
Router# show ip pim mdt bgp

MDT-default group 535151414
  rid:4141414 next_hop:4141414
```

[Table 2-63](#) describes the fields shown in the display.

**Table 2-63 show ip pim mdt bgp Field Descriptions**

Field	Description
MDT-default group	MDT default groups that have been advertised to this router.
rid:10.1.1.1	BGP router ID of the advertising router.
next_hop:10.1.1.1	BGP next-hop address that was contained in the advertisement.

# show ip pim mdt history

To display the information on data MDTs that have been reused, use the **show ip pim mdt history** command.

**show ip pim vrf** *vrf-name* **mdt history interval** *minutes*

Syntax Description	Parameter	Description
	<b>vrf</b> <i>vrf-name</i>	Specifies the name that is assigned to the multicast VRF instance.
	<b>interval</b> <i>minutes</i>	Specifies the length of time, in minutes, for which the interval can be configured; valid values are from 1 to 71582 minutes (the maximum is 71582 minutes or 7 weeks).

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **show ip pim mdt history** command displays the data MDTs that have been reused during the past configured interval.

**Examples** This example shows how to display the information on data MDTs that have been reused:

```
Router# show ip pim vrf blue mdt history interval 20

MDT-data send history for VRF - blue for the past 50 minutes

MDT-data group      Number of reuse
40191918             3
40191919             5
```

[Table 2-64](#) describes the fields shown in the display.

**Table 2-64 show ip pim mdt history Field Descriptions**

Field	Description
MDT-data group	MDT data group for which information is being shown.
Number of reuse	Number of data MDTs that have been reused in this group.

# show ip pim mdt receive

To display the data MDT advertisements that are received by a specified router, use the **show ip pim mdt receive** command.

**show ip pim vrf** *vrf-name* **mdt receive** [**detail**]

Syntax Description	
<b>vrf</b> <i>vrf-name</i>	Specifies the name that is assigned to the multicast VRF instance.
<b>detail</b>	(Optional) Provides a detailed description of the data MDT advertisements that are received.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** When a router wants to switch over from the default MDT to a data MDT, it advertises the VRF source, the group pair, and the global multicast address over which the traffic will be sent. If the remote router wants to receive this data, then the remote router joins this global address multicast group.

**Examples** This example shows how to display the data MDT advertisements that are received by a specified router:

```
Router# show ip pim vrf vpn8 mdt receive detail
```

```
Joined MDT-data groups for VRF:vpn8
group:535151810 source:4010101400 ref_count:43
(40140418140, 555141814), 4d43h/00:03:58/00:05:56, OIF count:4, flags:T\
(40140518140, 555141814), 4d43h/00:03:58/00:05:57, OIF count:4, flags:T\
```

[Table 2-65](#) describes the fields shown in the display.

**Table 2-65 show ip pim mdt receive Field Descriptions**

Field	Description
group:172.16.8.0	Group that caused the data MDT to be built.
source:10.0.0.100	VRF source that caused the data MDT to be built.
ref_count:13	Number of source and group pairs that are reusing this data MDT.

*Table 2-65 show ip pim mdt receive Field Descriptions (continued)*

Field	Description
OIF count:l	Number of interfaces out of which this multicast data is being forwarded.
flags:	Information about the entry: A - Candidate MSDP advertisement B - Bidir group D - Dense C - Connected F - Register flag I - Received source-specific host report J - Join SPT L - Local M - MSDP-created entry P - Pruned R - RP bit set S - Sparse s - SSM group T - SPT bit set X - Proxy join timer running U -URD Y - Joined MDT data group y - Sending to MDT data group Z - Multicast tunnel

# show ip pim mdt send

To display the data MDT advertisements that a specified router has made, use the **show ip pim mdt send** command.

**show ip pim vrf *vrf-name* mdt send**

Syntax Description	<b>vrf <i>vrf-name</i></b>	Specifies the name that is assigned to the multicast VRF instance.
--------------------	----------------------------	--

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Use this command to show the data MDT advertisements that a specified router has made.

**Examples** This example shows how to display the data MDT advertisements that a specified router has made:

```
Router# show ip pim mdt send

MDT-data send list for VRF:vpn8
  (source, group)           MDT-data group      ref_count
(40140018140, 555141814)   535151810           4
(40140018140, 555141815)   535151814           4
(40140018140, 555141813)   535151815           4
(40140018140, 555141814)   535151813           4
(40140018140, 555141815)   535151814           4
(40140018140, 555141816)   535151815           4
(40140018140, 555141817)   535151816           4
(40140018140, 555141818)   535151817           4
(40140018140, 555141819)   535151818           4
(40140018140, 5551418140)  535151819           4
```

Table 2-66 describes the fields shown in the display.

**Table 2-66** *show ip pim mdt send* Field Descriptions

Field	Description
source, group	Source and group addresses that this router has switched over to data MDTs.
MDT-data group	Multicast address over which these data MDTs are being sent.
ref_count	Number of source and group pairs that are reusing this data MDT.

# show ip pim neighbor

To display the list that the PIM neighbors discovered, use the **show ip pim neighbor** command.

```
show ip pim vrf vrf-name neighbor [interface-type interface-number]
```

Syntax Description	Parameter	Description
	<b>vrf</b> <i>vrf-name</i>	Specifies the name that is assigned to the multicast VRF instance.
	<i>interface-type</i>	(Optional) Interface type.
	<i>interface-number</i>	Interface number.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Use this command to determine which routers on the LAN are configured for PIM.

**Examples** This example shows how to display the list that the PIM neighbors discovered:

```
Router# show ip pim neighbor
```

```
PIM Neighbor Table
Neighbor Address  Interface      Uptime    Expires    Mode
495146813715     Ethernet0     47:38:46  0:04:55   Dense
4951468137133     Ethernet0     47:33:50  0:04:05   Dense (DR)
49514681361434     Ethernet4     47:33:50  0:04:08   Dense (DR)
49514681361430     Ethernet4     48:56:06  0:04:04   Dense
401415519         Tunnel0       49:44:59  0:04:09   Dense
```

[Table 2-67](#) describes the fields shown in the display.

**Table 2-67 show ip pim neighbor Field Descriptions**

Field	Description
Neighbor Address	IP address of the PIM neighbor.
Interface	Interface type and number on which the neighbor is reachable.
Uptime	Time in hours, minutes, and seconds that the entry has been in the PIM neighbor table.
Expires	Time in hours, minutes, and seconds until the entry will be removed from the IP multicast routing table.

Table 2-67 show ip pim neighbor Field Descriptions (continued)

Field	Description
Mode	Mode in which the interface is operating.
(DR)	Status of whether this neighbor is a designated router on the LAN.

## Related Commands

Command	Description
<b>ip pim state-refresh disable</b>	Disables the processing and forwarding of PIM dense-mode refresh-control messages on a PIM router.
<b>ip pim state-refresh origination-interval</b>	Configures the origination of and the interval for PIM dense-mode state-refresh control messages on a PIM router.
<b>show ip pim interface df</b>	Displays information about the designated forwarder interface.

# show ip pim rp-hash

To display which rendezvous point is being selected for a specified group, use the **show ip pim rp-hash** command.

```
show ip pim vrf vrf-name rp-hash {group-address | group-name}
```

## Syntax Description

<b>vrf</b> <i>vrf-name</i>	Specifies the name that is assigned to the multicast VRF instance.
<i>group-address</i> / <i>group-name</i>	Rendezvous-point information for the specified group address or name as defined in the DNS hosts table.

## Defaults

This command has no default settings.

## Command Modes

EXEC

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

This command displays which rendezvous point was selected for the group specified. It also shows whether this rendezvous point was selected by Auto-RP or the PIM Version 2 bootstrap mechanism.

## Examples

This example shows how to display which rendezvous point is being selected for a specified group:

```
Router# show ip pim rp-hash 239.1.1.1
RP 475146154145 (mt4-47a1cisco1com), v5
  Info source: 475146154145 (mt4-47a1cisco1com), via bootstrap
  Uptime: 05:45:33, expires: 00:05:04
```

[Table 2-68](#) describes the fields shown in the display.

**Table 2-68** show ip pim rp-hash Field Descriptions

Field	Description
RP 172.16.24.12 (mt1-47a.cisco.com), v2	Address of the rendezvous point for the group specified (239.1.1.1). The DNS name of the rendezvous point within the parentheses. If the address of the rendezvous point is not registered in the DNS, a question mark (?) is displayed. PIM Version 2 is configured.
Info source: 172.16.24.12 (mt1-47a.cisco.com), via bootstrap	System from which the router learned this rendezvous-point information and the DNS name of the source. The rendezvous point was selected by the bootstrap mechanism. In this case, the BSR is also the rendezvous point.
Uptime	Length of time (in hours, minutes, and seconds) that the router has known about this rendezvous point.
expires	Time (in hours, minutes, and seconds) after which the information about this rendezvous point expires. If the router does not receive any refresh messages in this time, it discards information about this rendezvous point.

# show ip pim rp mapping

To display the mappings for the PIM group to the active rendezvous points, use the **show ip pim rp mapping** command.

```
show ip pim vrf vrf-name rp mapping [rp-address]
```

## Syntax Description

<b>vrf</b> <i>vrf-name</i>	Specifies the name that is assigned to the multicast VRF instance.
<i>rp-address</i>	(Optional) Rendezvous-point IP address.

## Defaults

If you do not specify an *rp-address*, the mappings for all the active rendezvous points are displayed.

## Command Modes

EXEC

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Examples

This example shows how to display the mappings for the PIM group to the active rendezvous points:

```
Router# show ip pim rp mapping
PIM Group-to-RP Mappings
This system is an RP-mapping agent
Group(s) 554141010/46
RP 6161616 (?), v5v4
Info source: 6161616 (?), elected via Auto-RP ---> learned via Auto-RP
and the elected RP1
Uptime: 55:36:49, expires: 00:05:04
Group(s) 555151510/54
RP 9191919 (?), v5v4, bidir
Info source: 9191919 (?), elected via Auto-RP
Uptime: 55:36:50, expires: 00:05:37
Group(s) 556151510/54
RP 5151515 (?), v5v4, bidir
Info source: 5151515 (?), elected via Auto-RP
Uptime: 55:36:54, expires: 00:05:59
Group(s) 557151510/54
RP 9191919 (?), v5v4, bidir
Info source: 9191919 (?), elected via Auto-RP
Uptime: 55:36:54, expires: 00:05:35
Router#
```

Table 2-69 describes the fields that are shown in the example.

**Table 2-69** *show ip pim rp mapping* Field Descriptions

Field	Description
Info source	ACL number.
Static	Group-to-mapping information from the static rendezvous-point configuration.
Bidir Mode	Status of whether the rendezvous point is operating in bidirectional mode.
RP	Address of the rendezvous point for that group.
(?)	Status that shows no Domain Name System (DNS) name has been specified.

# show ip pim snooping

To display the information about IP PIM snooping, use the **show ip pim snooping** command.

## show ip pim snooping

```
show ip pim snooping vlan vlan-id [neighbor | mac-group | statistics | mroute [{src-ip | group-ip}]
```

Syntax Description	Parameter	Description
	<b>vlan</b> <i>vlan-id</i>	Displays information for a specific VLAN; valid values are from 1 to 4094.
	<b>neighbor</b>	(Optional) Displays information about the neighbor database.
	<b>mac-group</b>	(Optional) Displays information about the GDA database in Layer 2.
	<b>statistics</b>	(Optional) Displays information about the VLAN statistics.
	<b>mroute</b>	(Optional) Displays information about the mroute database.
	<i>src-ip</i>	(Optional) Source IP address.
	<i>group-ip</i>	(Optional) Group IP address.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the information about the global status:

```
Router# show ip pim snooping
Global runtime mode: Enabled
Global admin mode : Enabled
Number of user enabled VLANs: 4
User enabled VLANs: 40
Router#
```

This example shows how to display the information about a specific VLAN:

```
Router# show ip pim snooping vlan 10
3 neighbors (0 DR priority incapable, 0 Bi-dir incapable)
6 mroutes, 3 mac entries
DR is 4014014014
RP DF Set
Router#
```

This example shows how to display the information about the neighbor database for a specific VLAN:

```
Router# show ip pim snooping vlan 10 neighbor
IP Address      Mac address      Port Uptime/Expires  Flags
4014014015      000a1f3301344a  3/43 00:09:57/00:04:55
4014014014      000a1f3301334a  3/45 00:09:44/00:04:54
4014014014      000a1f33013c00  45/04 00:09:57/00:04:55 DR
Number of Neighbors = 3
Router#
```

This example shows how to display the information about the GDA database for a specific VLAN in Layer 2:

```
Router# show ip pim snooping vlan 10 mac-group
Mac address      Group address      Uptime/Expires      Outgoing Ports
040015e0416465  5541414001404      00:50:56/00:05:43  3/45 3/43 45/4
040015e0416464  5541414001400      00:50:58/00:05:44  3/45 3/43 45/4
040015e0010458  55410141410        00:50:57/00:05:47  3/45 3/43 45/4
Number of mac-groups = 3
Router#
```

This example shows how to display the detailed statistics for a specific VLAN:

```
Router# show ip pim snooping vlan 10 statistics
PIMv5 statistics for vlan 40:
Hello                                     : 844
Join/Prunes                               : 4335
RP DF Election                             : 0
Asserts                                    : 433
Other types                                : 0

Hello option holdtime [4]                  : 844
Hello option Generation ID[50]             : 544
Hello option DR priority[49]               : 544
Hello option Bi-dir capable[55]           : 0
Hello option Fast Hold[65005]              : 0
Hello option Lan Prune Delay[5]            : 0
Hello option Tag switching [47]            : 0
Hello option PIM-DM State Refresh[54]      : 544
Hello option Deprecated Cisco DR priority[48] : 0
Error - Hello length too short             : 0
Error - Hello hold option missing           : 0
Error - Hello option length                 : 0
Error - Hello option unknown                : 0

Error - Join/Prune Address Family           : 0
Error - Join/Prune Parser malloc failure    : 0
Error - Join/Prune Unknown up/down neighbor : 0
Error - Join/Prune Malformed packet discards : 0

Error - RPDF election Address Family        : 0
Error - RPDF Unknown up/down neighbor      : 0

Error - Generic packet input error          : 0
Router#
```

This example shows how to display the information about the mroute database for all mrouter in a specific VLAN:

```
Router# show ip pim snooping vlan 10 mroute
Number of Mroutes = 6
Flags: J/P - (*,G) Join/Prune, j/p - (S,G) Join/Prune
SGR-P - (S,G,R) Prune
```

## ■ show ip pim snooping

```

(*, 5541414001404), 00:46:44/00:05:58
 4014014014->4014014015, 00:46:44/00:05:58, J
  Downstream ports: 3/45
  Upstream ports: 3/43
  Outgoing ports: 3/45 3/43

(*, 5541414001400), 00:46:46/00:05:56
 4014014014->4014014015, 00:46:46/00:05:56, J
  Downstream ports: 3/45
  Upstream ports: 3/43
  Outgoing ports: 3/45 3/43

(4014014015, 5541014140), 00:46:40/00:03:03
 4014014014->4014014015, 00:46:40/00:03:03, SGR-P
  Downstream ports:
  Upstream ports: 3/43
  Outgoing ports: 3/43

(*, 5541014140), 00:46:46/00:03:05
 4014014014->4014014015, 00:46:46/00:03:05, J
  Downstream ports: 3/45
  Upstream ports: 3/43
  Outgoing ports: 3/45 3/43

(*, 554140140140), 00:05:53/00:04:06
  Downstream ports:
  Upstream ports:
  Outgoing ports: 3/45 3/43

(453145314531453, 554140140140), 00:05:53/00:04:06
 4014014014->4014014015, 00:05:53/00:04:06, j
  Downstream ports: 3/45
  Upstream ports: 3/43
  Outgoing ports: 3/45 3/43
Router#

```

This example shows how to display the information about the PIM mroute for a specific source address:

```

Router# show ip pim snooping vlan 10 mroute 224.1.100.100
(*, 5541414001400), 00:46:36/00:05:36
 4014014014->4014014015, 00:46:36/00:05:36, J
  Downstream ports: 3/45
  Upstream ports: 3/43
  Outgoing ports: 3/45 3/43
Router#

```

This example shows how to display the information about the PIM mroute for a specific source and group address:

```

Router# show ip pim snooping vlan 10 mroute 123.123.123.123 224.10.10.10
(453145314531453, 554140140140), 00:03:04/00:00:55
 4014014014->4014014015, 00:03:04/00:00:55, j
  Downstream ports: 3/45
  Upstream ports: 3/43
  Outgoing ports: 3/45 3/43
Router#

```

Related Commands	Command	Description
	<a href="#">ip pim snooping (global configuration mode)</a>	Enables PIM snooping globally.
	<a href="#">ip pim snooping (interface configuration mode)</a>	Enables PIM snooping on an interface.

# show ip rpf events

To display the triggered RPF statistics, use the **show ip rpf events** command.

**show ip rpf** [*vrf vrf-name*] **events**

<b>Syntax Description</b>	<b>vrf</b> <i>vrf-name</i> (Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
---------------------------	---

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

**Command Modes** EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the triggered RPF statistics:

```
Router# show ip rpf events
Last 45 triggered multicast RPF check events
RPF backoff delay: 500 msec
RPF maximum delay: 5 sec
DATE/TIME BACKOFF PROTOCOL EVENT RPF CHANGES
Jan 4 00:00:551643 500 msec EIGRP Route UP 0
Jan 4 00:00:071583 4000 sec Connected Route UP 0
Jan 4 00:00:061583 500 msec Connected Route UP 0
Router#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">ip multicast rpf backoff</a>	Sets the PIM-backoff interval.
	<a href="#">ip multicast rpf interval</a>	Sets the RPF consistency-check interval.

# show ip wccp

To display the WCCP statistics, use the **show ip wccp** command.

```
show ip wccp [{service-number | web-cache} [detail | view]]
```

Syntax Description		
	<i>service-number</i>	(Optional) Identification number of the cache engine service group being controlled by a router; valid values are from 0 to 99.
	<b>web-cache</b>	(Optional) Directs the router to display statistics for the web-cache service.
	<b>detail</b>	(Optional) Displays information for the router and all cache engines in the currently configured cluster.
	<b>view</b>	(Optional) Displays which other members of a particular service group have or have not been detected.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Use the **show ip wccp** *service-number* command to provide the “Total Packets Redirected” count. The “Total Packets Redirected” count is the number of flows, or sessions, that are redirected.

Use the **show ip wccp** *service-number* **detail** command to provide the “Packets Redirected” count. The “Packets Redirected” count is the number of flows, or sessions, that are redirected.

Use the **show ip wccp** **web-cache detail** command to provide an indication of how many flows, rather than packets, are using Layer 2 redirection.

For cache-engine clusters using Cisco cache engines, the reverse proxy *service-number* is indicated by a value of 99.

Use the **clear ip wccp** command to reset the counter for the “Packets Redirected” information.

For additional information on the IP WCCP commands, refer to the “Configuring Web Cache Services Using WCCP” section in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

**Examples** This example shows how to display the connected cache engine using Layer 2 redirection:

```
Router# show ip wccp web-cache detail
WCCP Cache-Engine information:
  IP Address:          401441414
  Protocol Version:    510
  State:               Usable
  Redirection:         L5
  Initial Hash Info:   FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

```

Assigned Hash Info:  FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                    FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                    FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
Hash Allotment:    556 (400100%)
Packets Redirected: 40573
Connect Time:     47:05:44

```

Table 2-70 describes the fields that are shown in the example.

**Table 2-70** *show ip wccp web-cache detail Command Output Fields*

Field	Description
WCCP Cache-Engine information	Header for the area that contains fields for the IP address and version of WCCP that is associated with the router that is connected to the cache engine in the service group.
IP Address	IP address of the router that is connected to the cache engine in the service group.
Protocol Version	Version of WCCP that is used by the router in the service group.
WCCP Cache-Engine information	Fields for information on cache engines.
IP Address	IP address of the cache engine in the service group.
Protocol Version	Version of WCCP that is used by the cache engine in the service group.
State	Status of whether the cache engine is operating properly and can be contacted by a router and other cache engines in the service group.
Initial Hash Info	Initial state of the hash-bucket assignment.
Assigned Hash Info	Current state of the hash-bucket assignment.
Hash Allotment	Percentage of buckets that is assigned to the current cache engine. Both a value and a percent figure are displayed.
Packets Redirected	Number of flows or sessions that have been redirected to the cache engine.
Connect Time	Amount of time that it takes for the cache engine to connect to the router.

#### Related Commands

Command	Description
<b>clear ip wccp</b>	Removes WCCP statistics (counts) maintained on the router for a particular service.
<b>ip wccp</b>	Directs a router to enable or disable the support for a cache engine service group.
<b>ip wccp redirect</b>	Enables packet redirection on an outbound or inbound interface using WCCP.
<b>ip wccp web-cache accelerated</b>	Enables the hardware acceleration for WCCP version 1.
<b>show ip interface</b>	Displays the usability status of interfaces that are configured for IP.

# show ipv6 mfib

To display the forwarding entries and interfaces in the IPv6 MFIB, use the **show ipv6 mfib** command.

```
show ipv6 mfib [{group-ip-addr/prefix-length | group-name | group-address [source-name |
source-address]} | {active kbps} | count | interface | status | summary | verbose]
```

```
show ipv6 mfib [link-local [active [kbps] | count | verbose]]
```

## Syntax Description

<i>group-ip-addr/prefix-length</i>	(Optional) Group IPv6 address/prefix length for the IPv6 network assigned to the interface.
<i>group-name</i>	(Optional) Multicast group name.
<i>group-address</i>	(Optional) Group IPv6 address.
<i>source-name</i>	(Optional) Source name.
<i>source-address</i>	(Optional) Source IP address.
<b>active</b> <i>kbps</i>	(Optional) Displays the rate at which active sources are sending to multicast groups; valid values are from 0 to 4294967295 kilobits per second.
<b>count</b>	(Optional) Displays information about the route and packet count.
<b>interface</b>	(Optional) Displays information about the interface settings and status.
<b>status</b>	(Optional) Displays information about the general settings and status.
<b>summary</b>	(Optional) Displays information about the summary statistics.
<b>verbose</b>	(Optional) Displays additional information such as the MAC encapsulation header and platform-specific information.
<b>link-local</b>	(Optional) Displays the link-local groups.

## Defaults

*prefix-length* is **128**.

## Command Modes

User EXEC or Privileged EXEC

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

Use the **show ipv6 mfib** command to display MFIB entries, forwarding interfaces, and their traffic statistics. This command can be enabled on virtual IP (VIP) if the router is operating in distributed mode.

Use the **show ipv6 mfib active** command to display MFIB entries actively used to forward packets. In many cases, it is useful to provide the optional *kbps* argument to display the set of entries that are forwarding an amount of traffic larger or equal to the amount set by the *kbps* argument.

Use the **show ipv6 mfib count** command to display the average packet size and data rate in kilobits per seconds.

The *prefix-length* is the length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

A forwarding entry in the MFIB has flags that determine the default forwarding and signaling behavior to use for packets matching the entry. The entry also has per-interface flags that further specify the forwarding behavior for packets received or forwarded on specific interfaces. [Table 2-71](#) describes the MFIB forwarding entries and interface flags.

**Table 2-71 MFIB Forwarding Entries and Interface Flags**

Flag	Description
F	Forward—Data is forwarded out of this interface.
A	Accept—Data received on this interface is accepted for forwarding.
IC	Internal copy—Deliver a copy of the packets received or forwarded on this interface to the router.
NS	Negate signal—Reverse the default entry signaling behavior for packets received on this interface.
DP	Do not preserve—When signaling the reception of a packet on this interface, do not preserve a copy of it (discard it instead).
SP	Signal present—The reception of a packet on this interface was just signaled.
S	Signal—By default, signal the reception of packets matching this entry.
C	Perform directly connected check for packets matching this entry. Signal the reception if packets were originated by a directly connected source.

## Examples

This example shows how to display information for a specific group IPv6 address:

```
Router# show ipv6 mfib ff35::1:1
IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
                 IC - Internal Copy, NP - Not platform switched
                 SP - Signal Present
Interface Counts: Distributed FS Pkt Count/FS Pkt Count/PS Pkt Count
(4600::5,FF35::4:4) Flags:
  RP Forwarding: 7488/400/48/37, Other: 503649/503649/0
  LC Forwarding: 0/0/0/0, Other: 0/0/0
  Vlan55 Flags: A
  Vlan44 Flags: F NS
  Pkts: 0/7488/0
```

Table 2-72 describes the fields shown in the display.

**Table 2-72 show ipv6 mfib Field Descriptions**

Field	Description
Entry flags	Information about the entry.
Forwarding Counts	Statistics on the packets that are received and forwarded to at least one interface.
Pkt Count/	Total number of packets received and forwarded since the creation of the multicast forwarding state to which this counter applies.
Pkts per second/	Number of packets received and forwarded per second.
Avg Pkt Size/	Total number of bytes divided by the total number of packets for this multicast forwarding state. There is no direct display for the total number of bytes. You can calculate the total number of bytes by multiplying the average packet size by the packet count.
Kbits per second	Bytes per second divided by packets per second, and divided by 1000.
Other counts:	Statistics on the received packets. These counters include statistics about the packets received and forwarded and packets received but not forwarded.
Interface Flags:	Information about the interface. See Table 2-71 for further information on interface flags.
Interface Counts:	Interface statistics.

This example shows forwarding entries and interfaces in the MFIB with a group address of FF03:1::1 and a source address of 5002:1::2 specified:

```
Router# show ipv6 mfib FF03:1::1 5002:1::2

IP Multicast Forwarding Information Base
Entry Flags:C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:Total/RPF failed/Other drops
Interface Flags:A - Accept, F - Forward, NS - Negate Signalling
                IC - Internal Copy, NP - Not platform switched
                SP - Signal Present
Interface Counts:FS Pkt Count/PS Pkt Count
(5005:4::5,FF03:4::4) Flags:
  Forwarding:74505/0/50/0, Other:45/0/45
  GigabitEthernet5/0 Flags:A
  GigabitEthernet5/0149 Flags:F NS
    Pkts:539/54
  GigabitEthernet5/0150 Flags:F NS
    Pkts:539/54
1
1
1
  GigabitEthernet5/0146 Flags:F NS
    Pkts:74658/54
```

This example shows forwarding entries and interfaces in the MFIB with a group address of FF03:1::1 and a default prefix of 128:

```
Router# show ipv6 mfib FF03:1::1/128

IP Multicast Forwarding Information Base
Entry Flags:C - Directly Connected, S - Signal, IA - Inherit A flag,
```

```

          AR - Activity Required, D - Drop
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:Total/RPF failed/Other drops
Interface Flags:A - Accept, F - Forward, NS - Negate Signalling
                IC - Internal Copy, NP - Not platform switched
                SP - Signal Present
Interface Counts:FS Pkt Count/PS Pkt Count
(*,FF03:4::4) Flags:C
  Forwarding:0/0/0/0, Other:0/0/0
  Tunnel4 Flags:A NS
  GigabitEthernet5/0155 Flags:F NS
    Pkts:0/0
1
1
1
  GigabitEthernet5/0146 Flags:F NS
    Pkts:0/0

```

This example displays statistics on the rate at which active IP multicast sources are sending information. The router is switching traffic from 2001::1:1:200 to FF05::1:

```

Router# show ipv6 mfib active

Active IPv6 Multicast Sources - sending >= 4 kbps
Group: FF05::4
  Source: 5004::4:4:500
    Rate: 50 pps/46 kbps(4sec), 0 kbps(last 458 sec)

```

Table 2-73 describes the fields shown in the display.

**Table 2-73 show ipv6 mfib active Field Descriptions**

Field	Description
Group:	Summary information about counters for (*, G) and the range of (S,G) states for one particular group G. The following RP-tree: and Source: output fields contain information about the individual states belonging to this group.  <b>Note</b> For PIM-SSM range groups, the Group: displays are statistical. All SSM range (S,G) states are individual, unrelated SSM channels.
Rate...kbps	Bytes per second divided by packets per second and divided by 1000. On an IP multicast fast-switching platform, the number of packets per second is the number of packets during the last second. Other platforms may use a different approach to calculate this number. Refer to the <i>Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY</i> for more information.

This example displays statistics from the MFIB about the group and source. The router is switching traffic from 2001::1:1:200 to FF05::1:

```

Router# show ipv6 mfib count

IP Multicast Statistics
54 routes, 7 groups, 0144 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: FF00::/8
  RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0
Group: FF00::/45
  RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0

```

```

Group: FF05::4
  RP-tree: Forwarding: 5/0/400/0, Other: 0/0/0
  Source: 40::4:4:500, Forwarding: 367/40/400/7, Other: 0/0/0
  Totl shown: Source count: 4, pkt count: 369
Group: FF40::/45
  RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0
Group: FF50::/45
  RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0

```

Table 2-74 describes the fields shown in the display.

**Table 2-74** show ipv6 mfib count Field Descriptions

Field	Description
Forwarding Counts	Statistics on the packets that are received and forwarded to at least one interface.
Pkt Count/	Total number of packets received and forwarded since the multicast forwarding state to which this counter applies was created.
Pkts per second/	Number of packets received and forwarded per second.
Avg Pkt Size/	Total number of bytes divided by the total number of packets for this multicast forwarding state. There is no direct display for the total number of bytes. You can calculate the total number of bytes by multiplying the average packet size by the packet count.
Kilobits per second	Bytes per second, divided by packets per second, and divided by 1000.
Other counts:	Statistics on the received packets. These counters include statistics about the packets received and forwarded and packets received but not forwarded.
Total/	Total number of packets received.
RPF failed/	Number of packets not forwarded due to a failed RPF or acceptance check (when bidirectional PIM is configured).
Other drops (OIF-null, rate-limit etc)	Number of packets not forwarded for reasons other than an RPF or acceptance check (such as the outgoing interface [OIF] list was empty or because the packets were discarded because of a configuration that was enabled).
Group:	Summary information about counters for (*,G) and the range of (S,G) states for one particular group G. The following RP-tree: and Source: output fields contain information about the individual states belonging to this group.  <b>Note</b> For Source Specific Multicast (PIM-SSM) range groups, the Group: displays are statistical. All SSM range (S,G) states are individual, unrelated SSM channels.
RP-tree:	Counters for the (*,G) state of this group G. These counters are displayed only for groups that have a forwarding mode that do not forward packets on the shared tree. These (*,G) groups are bidirectional PIM and PIM sparse mode (PIM-SM) groups. There are no RP-tree displays for PIM SSM range groups.

This example shows forwarding entries and interfaces in the MFIB and additional information such as the MAC encapsulation header and platform-specific information:

```

Router# show ipv6 mfib ff33::1:1 verbose
IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, K - Keepalive
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops

```

```

Platform per slot HW-Forwarding Counts: Pkt Count/Byte Count
Platform flags: HF - Forwarding entry,HB - Bridge entry,HD - NonRPF Drop entry,
                NP - Not platform switchable,RPL - RPF-1tl linkage,
                MCG - Metset change,ERR - S/w Error Flag,RT\ - In RetryQ,
                LP - L3 pending,MP - Met pending,AP - ACL pending
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
                IC - Internal Copy, NP - Not platform switched
                SP - Signal Present
Interface Counts: Distributed FS Pkt Count/FS Pkt Count/PS Pkt Count
(40::5,FF33::4:4) Flags: K
  RP Forwarding: 0/0/0/0, Other: 0/0/0
  LC Forwarding: 0/0/0/0, Other: 0/0/0
  HW Forwd:    0/0/0/0, Other: NA/NA/NA
  Slot 6: HW Forwarding: 0/0, Platform Flags:  HF RPL
  Slot 4: HW Forwarding: 0/0, Platform Flags:  HF RPL
  Vlan40 Flags: A
  Vlan30 Flags: F NS
  Pkts: 0/0/0 MAC: 33330004000400D0FFFE480086DD
Router#

```

Table 2-75 describes the fields shown in the display.

**Table 2-75 show ipv6 mfib verbose Field Descriptions**

Field	Description
Platform flags	Information about the platform.
Platform per slot HW-Forwarding Counts	Total number of packets per bytes forwarded.

Table 2-76 describes the MFIB platform flags.

**Table 2-76 MFIB Platform Flags**

Flag	Description
H	Entry is installed in hardware
HF	Forwarding entry
HB	Bridge entry
HD	NonRPF Drop entry
NP	Software switched
RPL	RPF-1tl linkage
MCG	Metset change
ERR	S/w Error Flag
RTY	In RetryQ
LP	Layer 3 pending
MP	Met pending
AP	ACL pending

# show ipv6 mld snooping

To display MLDv2 snooping information, use the **show ipv6 mld snooping** command.

```
show ipv6 mld snooping { {explicit-tracking vlan} | {mrouter [vlan vlan]} | {report-suppression
vlan vlan} | {statistics vlan vlan} }
```

Syntax Description		
<b>explicit-tracking vlan</b> <i>vlan</i>		Displays the status of explicit host tracking.
<b>mrouter</b>		Displays the multicast router interfaces on an optional VLAN.
<b>vlan</b> <i>vlan</i>		(Optional) Specifies the VLAN number on the multicast router interfaces.
<b>report-suppression vlan</b> <i>vlan</i>		Displays the status of the report suppression.
<b>statistics vlan</b> <i>vlan</i>		Displays IGMP snooping information on a VLAN.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** You can also use the **show ip igmp snooping** commands to display information about IGMP snooping. You can enter the **show ipv6 mld snooping mrouter** command without arguments to display all the multicast router interfaces.

**Examples** This example shows how to display explicit tracking information on VLAN 25:

```
Router# show ipv6 mld snooping explicit-tracking vlan 25
Source/Group          Interface    Reporter    Filter_mode
-----
40141414/556151515    V155:4/5    461571513   INCLUDE
40151515/556151515    V155:4/5    461571513   INCLUDE
Router#
```

This example shows how to display the multicast router interfaces in VLAN 1:

```
Router# show ipv6 mld snooping mrouter vlan 1
vlan          ports
-----+-----
4             Gi4/4, Gi5/4, Fa3/48, Router
Router#
```

## ■ show ipv6 mld snooping

This example shows the IGMP snooping statistics information for VLAN 25:

```
Router# show ipv6 mld snooping statistics interface vlan 25
```

```
Snooping statistics for Vlan55
#channels:5
#hosts :4
```

Source/Group	Interface	Reporter	Uptime	Last-Join	Last-Leave
40141414/556151515	Gi4/5:V155	461571513	00:04:47	00:00:50	-
40151515/556151515	Gi4/5:V155	461571513	00:04:47	00:00:50	-

```
Router#
```

## Related Commands

Command	Description
<a href="#">ipv6 mld snooping</a>	Enables MLDv2 snooping globally.
<a href="#">ipv6 mld snooping explicit-tracking</a>	Enables explicit host tracking.
<a href="#">ipv6 mld snooping querier</a>	Enables the MLDv2 snooping querier.
<a href="#">ipv6 mld snooping report-suppression</a>	Enables report suppression on a VLAN.

# show l2protocol-tunnel

To display the protocols that are tunneled on an interface or on all interfaces, use the **show l2protocol-tunnel** command.

```
show l2protocol-tunnel [{interface interface mod/port} | {vlan vlan-id} | summary]
```

Syntax Description	Parameter	Description
	<b>interface</b> <i>interface</i>	(Optional) Specifies the interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , <b>atm</b> , and <b>ge-wan</b> .
	<i>mod/port</i>	Module and port number.
	<b>vlan</b> <i>vlan-id</i>	Specifies the VLAN; valid values are from 1 to 4094.
	<b>summary</b>	(Optional) Displays a summary of a tunneled port.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **show l2protocol-tunnel** command displays only the ports that have protocol tunneling enabled. The **show l2protocol-tunnel summary** command displays the ports that have protocol tunneling enabled, regardless of whether the port is down or currently configured as a trunk.

**Examples** This example shows how to display the protocols that are tunneled on all interfaces:

```
Router# show l2protocol-tunnel
COS for Encapsulated Packets: 5
Drop Threshold for Encapsulated Packets: 3000
Port      Protocol Shutdown      Drop      Encapsulation Decapsulation      Drop
          Threshold Threshold Counter      Counter      Counter
-----
Fa3/38   cdp      ----      3000      5           0           0
          stp      ----      3000      5653        0           0
          ---      ----      ----      ----        ----        ----
Router#
```

This example shows how to display a summary of Layer 2-protocol tunnel ports:

```
Router# show l2protocol-tunnel summary
COS for Encapsulated Packets:5
Drop Threshold for Encapsulated Packets:0

Port      Protocol      Shutdown      Drop      Status
          Threshold
          (cdp/stp/vtp)      (cdp/stp/vtp)
```

```
show l2protocol-tunnel
```

```
-----
Fa9/4   --- stp --- ----/----/----  ----/----/----  down
Fa9/9   cdp stp vtp ----/----/----  ----/----/----  up
Fa9/47  --- --- --- ----/----/----  4500/4500/4500  down (trunk)
Fa9/48  cdp stp vtp ----/----/----  ----/----/----  down (trunk)
Router>
```

---

**Related Commands**

Command	Description
<b>l2protocol-tunnel</b>	Enables the protocol tunneling on an interface and specifies the type of protocol to be tunneled.
<b>l2protocol-tunnel drop-threshold</b>	Specifies the maximum number of packets that can be processed for the specified protocol on that interface before being dropped.
<b>l2protocol-tunnel global drop-threshold</b>	Enables rate limiting at the software level.
<b>l2protocol-tunnel shutdown-threshold</b>	Specifies the maximum number of packets that can be processed for the specified protocol on that interface in 1 second.

# show l3-mgr

To display the information about the Layer 3 manager, use the **show l3-mgr** command.

## show l3-mgr status

```
show l3-mgr {interface {{interface interface-number} | {null interface-number} |
{port-channel number} | {vlan vlan-id} | status}}
```

Syntax	Description
<b>status</b>	Displays information about the global variable.
<b>interface</b>	Displays information about the Layer 3 manager.
<i>interface</i>	Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , <b>atm</b> , and <b>ge-wan</b> .
<i>interface-number</i>	Module and port number; see the “Usage Guidelines” section for valid values.
<b>null</b> <i>interface-number</i>	Specifies the null interface; the valid value is <b>0</b> .
<b>port-channel</b> <i>number</i>	Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 282.
<b>vlan</b> <i>vlan-id</i>	Specifies the VLAN; valid values are from 1 to 4094.
<b>status</b>	Displays status information about the Layer 3 manager.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The **port-channel** *number* values from 257 to 282 are supported on the CSM and the FWSM only.

**Examples** This example shows how to display the status of the Layer 3 manager:

```
Router# show l3-mgr status
l3_mgr_state:      5
l3_mgr_req_q1count: 0
l3_mgr_req_q1head: 0
```

```
l3_mgr_req_q1tail:    0
l3_mgr_max_queue_count: 4060
l3_mgr_shrunk_count:  0
l3_mgr_req_qlip_inv_count: 303
l3_mgr_req_qlipx_inv_count: 0
l3_mgr_outpak_count: 48874
l3_mgr_inpak_count:  48874

l3_mgr_max_pending_pak: 4
l3_mgr_pending_pak_count: 0

nde enable statue:    0
current nde addr:    0101010
```

Router#

This example shows how to display the information about the Layer 3 manager for a specific interface:

```
Router# show l3-mgr interface fastethernet 5/40
vlan:                0
ip_enabled:          4
ipx_enabled:         4
bg_state:            0 0 0 0
hsrp_enabled:        0
hsrp_mac:            00001000010000
state:               0
up:                  0
Router#
```

# show lacp

To display LACP information, use the **show lacp** command.

```
show lacp [channel-group] { counters | internal | neighbors | sys-id }
```

Syntax Description	
<i>channel-group</i>	(Optional) Number of the channel group; valid values are from 1 to 282.
<b>counters</b>	Displays information about the LACP statistics.
<b>internal</b>	Displays LACP internal information.
<b>neighbors</b>	Displays information about the LACP neighbor.
<b>sys-id</b>	Displays the LACP system identification.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** If you do not specify a *channel-group*, all channel groups are displayed. The *channel-group* values from 257 to 282 are supported on the CSM and the FWSM only. You can enter the optional *channel-group* to specify a channel group for all keywords, except the **sys-id** keyword.

**Examples** This example shows how to display the LACP statistics for a specific channel group:

```
Router# show lacp 1 counters
          LACPDUs      Marker      LACPDUs
Port      Sent  Recv      Sent  Recv      Pkts Err
-----
Channel group: 4
  Fa4/4    8    45        0    0         3    0
  Fa4/5   44   48        0    0         3    0
  Fa4/3   44   48        0    0         0
  Fa4/4   43   48        0    0         0
```

The output displays the following information:

- The LACPDUs Sent and Recv columns display the LACPDUs that are sent and received on each specific interface.
- The LACPDUs Pkts and Err columns display the marker-protocol packets.

This example shows how to display internal information for the interfaces that belong to a specific channel:

```
Router# show lacp 1 internal
Flags: S - Device sends PDUs at slow rate1 F - Device sends PDUs at fast rate1
       A - Device is in Active mode1       P - Device is in Passive mode1

Channel group 4

Port      Flags   State   LACPDU   LACP Port  Admin  Oper   Port   Port
         Interval Priority  Key      Key      Number State
Fa4/4    saC     bndl    30s      35768     400    400    0xc4   0x75
Fa4/5    saC     bndl    30s      35768     400    400    0xc5   0x75
Fa4/3    saC     bndl    30s      35768     400    400    0xc3   0x75
Fa4/4    saC     bndl    30s      35768     400    400    0xc4   0x75
Router#
```

Table 2-77 describes the fields that are shown in the example.

**Table 2-77 show lacp internal Command Output Fields**

Field	Description
State	State of the specific port at the current moment is displayed; allowed values are as follows: <ul style="list-style-type: none"> <li><i>bndl</i>—Port is attached to an aggregator and bundled with other ports.</li> <li><i>susp</i>—Port is in a suspended state; it is not attached to any aggregator.</li> <li><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).</li> <li><i>hot-sby</i>—Port is in a hot-standby state.</li> <li><i>down</i>—Port is down.</li> </ul>
LACPDU's 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 that are encoded as individual bits within a single octet with the following meaning [1]: <ul style="list-style-type: none"> <li><b>bit0</b>: <i>LACP_Activity</i></li> <li><b>bit1</b>: <i>LACP_Timeout</i></li> <li><b>bit2</b>: <i>Aggregation</i></li> <li><b>bit3</b>: <i>Synchronization</i></li> <li><b>bit4</b>: <i>Collecting</i></li> <li><b>bit5</b>: <i>Distributing</i></li> <li><b>bit6</b>: <i>Defaulted</i></li> <li><b>bit7</b>: <i>Expired</i></li> </ul>

This example shows how to display the information about the LACP neighbors for a specific port channel:

```
Router# show lacp 1 neighbors
Flags: S - Device sends PDUs at slow rate1 F - Device sends PDUs at fast rate1
      A - Device is in Active mode1      P - Device is in Passive mode1

Channel group 4 neighbors

Port      Partner
System ID Partner
Port Number Age  Flags
Fa4/4     8000,00b01c53e1d84e 0x84 59s P
Fa4/5     8000,00b01c53e1d84e 0x85 0s  P
Fa4/3     8000,00b01c53e1d84e 0x83 0s  P
Fa4/4     8000,00b01c53e1d84e 0x84 0s  P

      Port      Admin Oper      Port
Priority Key    Key    State
Fa4/4     35768 500    500    0x84
Fa4/5     35768 500    500    0x84
Fa4/3     35768 500    500    0x84
Fa4/4     35768 500    500    0x84
Router#
```

If no PDUs have been received, the default administrative information is displayed in braces.

This example shows how to display the LACP system identification:

```
Router> show lacp sys-id
8000,AC-45-34-56-78-90
```

The system identification is made up of the system priority and the system MAC address. The first 2 bytes are the system priority, and the last 6 bytes are the globally administered individual MAC address that is associated to the system.

#### Related Commands

Command	Description
<a href="#">clear lacp counters</a>	Clears the statistics for all interfaces belonging to a specific channel group.
<a href="#">lacp port-priority</a>	Sets the priority for the physical interfaces.
<a href="#">lacp system-priority</a>	Sets the priority of the system.

# show logging ip access-list

To display information about the logging IP access list, use the **show logging ip access-list** command.

**show logging ip access-list {cache | config}**

Syntax Description	cache	Displays information about all the entries in the OAL cache.
	config	Displays information about the logging IP access-list configuration.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** OAL is supported on IPv4 unicast traffic only.

**Examples** This example shows how to display all the entries in the OAL cache:

```
Router# show logging ip access-list cache
Matched flows:
id prot src_ip dst_ip sport dport status count
total lastlog
-----
4 47 501514185 541514515 444 63 Permit 0
3906 5d05h
5 47 501514185 541514515 4435 63 Permit 0
3906 5d05h
3 47 501514185 541514515 5459 63 Permit 0
3906 5d05h
4 47 501514185 541514515 3483 63 Permit 0
3906 5d05h
5 47 501514185 541514515 4507 63 Permit 0
3906 5d05h
6 47 501514185 541514515 5534 63 Deny 0
3906 5d05h
7 47 501514185 541514515 6555 63 Deny 0
3906 5d05h
8 47 501514185 541514515 7579 63 Permit 0
3906 5d05h
9 47 501514185 541514515 8303 63 Permit 0
3906 5d05h
40 47 501514185 541514515 9357 63 Permit 0
3905 5d05h
44 47 501514185 541514515 40354 63 Permit 0
3905 5d05h
```

```

45 47 501514185 541514515 44375 63 Permit 0
3905 5d05h
43 47 501514185 541514515 45399 63 Deny 0
3905 5d05h
44 47 501514185 541514515 43453 63 Permit 0
3905 5d05h
45 47 501514185 541514515 44447 63 Deny 0
3905 5d05h
46 47 501514185 541514515 45474 63 Permit 0
3905 5d05h
47 47 501514185 541514515 46495 63 Permit 0
3905 5d05h
48 47 501514185 541514515 47549 63 Permit 0
3905 5d05h
49 47 501514185 541514515 48543 63 Permit 0
3905 5d05h
50 47 501514185 541514515 49567 63 Permit 0
3905 5d05h

```

```

Number of entries: 50
Number of messages logged: 445
Number of packets logged: 44500
Number of packets received for logging: 44500
Router#

```

This example shows how to display information about the logging IP access-list configuration:

```

Router# show logging ip access-list config
Logging ip access-list configuration
Maximum number of cached entries: 8495
Logging rate limiter: 0
Log-update interval: 300
Log-update threshold: 0
Configured on input direction:
    Vlan5
    Vlan4
Configured on output direction:
    Vlan5
Router#

```

#### Related Commands

Command	Description
<a href="#">clear logging ip access-list cache</a>	Clears all the entries from the OAL cache and sends them to the syslog.
<a href="#">logging ip access-list cache (global configuration mode)</a>	Configures the OAL parameters.
<a href="#">logging ip access-list cache (interface configuration mode)</a>	Enables an OAL-logging cache on an interface that is based on direction.

## show mac-address-table

To display the information about the MAC-address table, use the **show mac-address-table** command.

**show mac-address-table**

**show mac-address-table** {*address mac-addr*} [**all** | {**interface** *interface interface-number*} | {**vlan** *vlan-id*}]

**show mac-address-table aging-time** [**vlan** *vlan-id*]

**show mac-address-table count** [**vlan** *vlan-id*]

**show mac-address-table dynamic** [{*address mac-addr*} | {**interface** *interface interface-number*} | {**vlan** *vlan-id*}]

**show mac-address-table** {**interface** *interface interface-number*}

**show mac-address-table limit** [**vlan** *vlan-id* | {**interface** *interface*}]

**show mac-address-table multicast** [**count** | {{**igmp-snooping** | **mld-snooping**} [**count**]}] | {**user** [**count**]} | {**vlan** *vlan-id*}]

**show mac-address-table notification** {**mac-move** | **threshold**}

**show mac-address-table static** [{*address mac-addr*} | **detail** | {**interface** *interface interface-number*} | {**vlan** *vlan-id*}]

**show mac-address-table synchronize statistics**

**show mac-address-table unicast-flood**

**show mac-address-table vlan** *vlan-id*

Syntax Description		
<b>address</b> <i>mac-addr</i>		Displays information about the MAC-address table for a specific MAC address; see the “Usage Guidelines” section for format guidelines.
<b>all</b>		(Optional) Displays every instance of the specified MAC address in the forwarding table.
<b>interface</b> <i>interface</i>		(Optional) Displays information about a specific interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , <b>atm</b> , and <b>ge-wan</b> .
<i>interface-number</i>		Module and port number; see the “Usage Guidelines” section for valid values.
<b>vlan</b> <i>vlan-id</i>		(Optional) Displays information for a specific VLAN only; valid values are from 1 to 4094.
<b>aging-time</b>		Displays information about the MAC-address aging time.
<b>count</b>		Displays the number of entries that are currently in the MAC-address table.
<b>dynamic</b>		Displays information about the dynamic MAC-address table entries only.

<b>limit</b>	Displays MAC-usage information.
<b>multicast</b>	Displays information about the multicast MAC-address table entries only.
<b>igmp-snooping</b>	Displays the addresses learned by IGMP snooping.
<b>mld-snooping</b>	Displays the addresses learned by MLDv2 snooping.
<b>user</b>	Displays the manually entered (static) addresses.
<b>notification mac-move</b>	Displays the MAC-move notification status.
<b>notification threshold</b>	Displays the CAM-table utilization notification status.
<b>static</b>	Displays information about the static MAC-address table entries only.
<b>synchronize statistics</b>	Displays information about the statistics collected on the switch processor.
<b>unicast-flood</b>	Displays unicast-flood information.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC

**Command History**

Release	Modification
12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

If you do not specify a module number, the output of the **show mac-address-table** command displays information about the supervisor engine. To display information about the MAC-address table of the switch processor, you must enter the **all** keyword.

The *mac-addr* is a 48-bit MAC address and the valid format is H.H.H.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

Valid values for *mac-group-address* are from 1 to 9.

The optional **count** keyword displays the number of multicast entries.

The optional **multicast** keyword displays the multicast MAC addresses (groups) in a VLAN or displays all statically installed or IGMP snooping-learned entries in the Layer 2 table.

The information that is displayed in the **show mac-address-table unicast-flood** command output is as follows:

- Up to 50 flood entries, shared across all the VLANs that are not configured to use the filter mode, can be recorded.

- The output field displays are defined as follows:
  - ALERT—Information is updated approximately every 3 seconds.
  - SHUTDOWN—Information is updated approximately every 3 seconds.



**Note** The information displayed on the destination MAC addresses is deleted as soon as the floods stop after the port shuts down.

- Information is updated each time that you install the filter. The information lasts until you remove the filter.

The **show mac-address-table protocol {assigned | ip | ipx | other}** syntax is not supported on Catalyst 6500 series switches that are configured with a Supervisor Engine 720.

The keyword definitions for the *protocol* argument are as follows:

- **assigned** specifies assigned protocol entries.
- **ip** specifies IP protocol.
- **ipx** specifies IPX protocols.
- **other** specifies other protocol entries.

The dynamic entries that are displayed in the Learn field are always set to Yes.

The **show mac-address-table limit** command output displays the following information:

- The current number of MAC addresses.
- The maximum number of MAC entries that are allowed.
- The percentage of usage.

The **show mac-address-table synchronize statistics** command output displays the following information:

- Number of messages processed at each time interval.
- Number of active entries sent for synchronization.
- Number of entries updated, created, ignored, or failed.

## Examples



### Note

In a distributed EARL switch, the asterisk (\*) indicates a MAC address that is learned on a port that is associated with this EARL.

This example shows how to display the information about the MAC-address table for a specific MAC address (the Catalyst 6500 series switch is configured with a Supervisor Engine 2):

```
Router# show mac-address-table address 001.6441.60ca
```

```
Codes: * - primary entry
```

```

vlan  mac address      type  learn qos      ports
-----+-----+-----+-----+-----
Supervisor:
* --- 000416444160ca   static No  -- Router
Router#
```

This example shows how to display MAC-address table information for a specific MAC address (the Catalyst 6500 series switch is configured with a Supervisor Engine 720):

```
Router# show mac-address-table address 0100.5e00.0128
Legend: * - primary entry
        age - seconds since last seen
        n/a - not available

      vlan  mac address      type   learn   age           ports
-----+-----+-----+-----+-----+-----
Supervisor:
*   44  040015e0010458      static \es           -   Fa6/44,Router
*    4  040015e0010458      static \es           -   Router
Module 9:
*   44  040015e0010458      static \es           -   Fa6/44,Router
*    4  040015e0010458      static \es           -   Router
Router#
```

This example shows how to display the currently configured aging time for all VLANs:

```
Router# show mac-address-table aging-time
Vlan   Aging Time
----   -
*400   300
500    4000

Router#
```

This example shows how to display the entry count for a specific slot:

```
Router# show mac-address-table count slot 1
MAC Entries on slot 4 :
Dynamic Address Count:           4
Static Address (User-defined) Count: 55
Total MAC Addresses In Use:      59
Total MAC Addresses Available:   434075
Router#
```

This example shows how to display all the dynamic MAC-address entries:

```
Router# show mac-address-table dynamic
Legend: * - primary entry
        age - seconds since last seen
        n/a - not applicable

      vlan  mac address      type   learn   age           ports
-----+-----+-----+-----+-----+-----
*   40  00401000010000      dynamic \es   n/a       Gi4/4
*    3  00401000010000      dynamic \es    0       Gi4/5
*    4  00051fcbclac64      dynamic \es  565      Gi8/4
*    4  0009145e91adc0      static  No    -         Router
Router#
```

This example shows how to display the information about the MAC-address table for a specific interface (the Catalyst 6500 series switch is configured with a Supervisor Engine 720):

```
Router# show mac-address-table interface fastethernet 6/45
Legend: * - primary entry
        age - seconds since last seen
        n/a - not available

      vlan  mac address      type   learn   age           ports
-----+-----+-----+-----+-----+-----
*   45  00e01f74c1845d      dynamic \es           5   Fa6/45
Router#
```

**Note**

A leading asterisk (\*) indicates entries from a MAC address that was learned from a packet coming from an outside device to a specific module.

This example shows how to display the MAC-move notification status:

```
Router# show mac-address-table notification mac-move
MAC Move Notification: Enabled
Router#
```

This example shows how to display the CAM-table utilization-notification status:

```
Router# show mac-address-table notification threshold
Status limit Interval
-----+-----+-----
enabled 4 450
Router#
```

This example shows how to display unicast-flood information:

```
Router# show mac-address-table unicast-flood
Unicast Flood Protection status: enabled
```

Configuration:

```
vlan Kfps action timeout
```

```
-----+-----+-----+-----
5 5 alert none
```

Mac filters:

```
No1 vlan souce mac addr1 installed
```

```
on time left (mm:ss)
```

```
-----+-----+-----+-----
```

Flood details:

```
Vlan souce mac addr1 destination mac addr1
```

```
-----+-----+-----+-----
5 0000100001cafe 0000100001bad0, 0000100001babe,
0000100001bac0
0000100001bac5, 0000100001bac4,
0000100001bac6
0000100001bac8
5 0000100001caff 0000100001bad4, 0000100001babf,
0000100001bac4
0000100001bac3, 0000100001bac5,
0000100001bac7
0000100001bac9
Router#
```

This example shows how to display all the static MAC-address entries (this Catalyst 6500 series switch is configured with a Supervisor Engine 2):

```
Router# show mac-address-table static
```

Codes: \* - primary entry

```
   vlan   mac address   type   learn qos   ports
-----+-----+-----+-----
* --- 000416444160ca   static No   -- Router
```

```
Router#
```

This example shows how to display the information about the MAC-address table for a specific VLAN:

```
Router# show mac-address-table vlan 100
vlan  mac address      type      protocol  qos      ports
-----+-----+-----+-----+-----+-----
400  005013e8d16400  static  assigned  --      Router
400  00501734510cff  dynamic         ip  --      Fa5/9
400  008014c9318040  dynamic         ip  --      Fa5/9
400  005013e8d16400  static         ipx  --      Router
400  005013e8d16400  static         other --      Router
400  040010cdd1dddd  static         other --      Fa5/9,Router,Switch
400  00d0158701a4ff  dynamic         ip  --      Fa5/9
400  00e014fac1b400  dynamic         ip  --      Fa5/9
400  040015e0010004  static         ip  --      Fa5/9,Switch
400  005013e8d16400  static         ip  --      Router
Router#
```

This example shows how to display the information about the MAC-address table for MLDv2 snooping:

```
Router# show mac-address-table multicast mld-snooping
vlan mac address type learn qos ports
-----+-----+-----+-----+-----+-----
--- 33331000010004 static \es - Switch,Stby-Switch
--- 3333100001000d static \es - Fa5/4, Fa4/4, Router, Switch
--- 33331000010046 static \es - Switch,Stby-Switch
Router#
```

#### Related Commands

Command	Description
<a href="#">mac-address-table aging-time</a>	Configures the aging time for entries in the Layer 2 table.
<a href="#">mac-address-table limit</a>	Enables MAC limiting.
<a href="#">mac-address-table notification mac-move</a>	Enables MAC-move notification.
<a href="#">mac-address-table static</a>	Adds static entries to the MAC-address table or configures a static MAC address with IGMP snooping disabled for that address.
<a href="#">mac-address-table synchronize</a>	Synchronizes the Layer 2 MAC address table entries across the PFC.

# show mac-address-table learning

To display the MAC-address learning state, use the **show mac-address-table learning** command.

```
show mac-address-table learning [{vlan vlan-id] | {interface interface slot/port}] [module num]
```

Syntax Description		
<b>vlan</b> <i>vlan-id</i>	(Optional) Displays information about the MAC-address learning state for the specified switch port VLAN; valid values are from 1 to 4094.	
<b>interface</b> <i>interface slot/port</i>	(Optional) Displays information about the MAC-address learning state for the specified routed interface type, the slot number, and the port number.	
<b>module</b> <i>num</i>	(Optional) Displays information about the MAC-address learning state for the specified module number.	

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

The **module** *num* keyword and argument can be used to specify supervisor engines only.

The **interface** *interface slot/port* keyword and arguments can be used on routed interfaces only. The **interface** *interface slot/port* keyword and arguments cannot be used to configure learning on switch-port interfaces.

If you specify the **vlan** *vlan-id*, the state of the MAC-address learning of the specified VLAN, including router interfaces, on all modules, is displayed.

If you specify the **vlan** *vlan-id* and the **module** *num*, the state of the MAC-address learning of a specified VLAN on a specified module is displayed.

If you specify the **interface** *interface slot/port* keyword and arguments, the state of the MAC-address learning of the specified interface on all modules is displayed.

If you specify the **interface** *interface slot/port* keyword and arguments, the state of the MAC-address learning of the specified interface on the specified module is displayed.

If you enter the **show mac-address-table learning** command with no arguments or keywords, the status of MAC learning on all the existing VLANs on all the supervisor engines configured on a Catalyst 6500 series switch is displayed.

**Examples**

This example shows how to display the MAC-address learning status on all the existing VLANs on all the supervisor engines:

```
Router# show mac-address-table learning

VLAN/Interface      Mod4   Mod4   Mod7
-----
4                   yes    yes    yes
400                 yes    yes    yes
450                 yes    yes    yes
500                 yes    yes    yes
550                 yes    yes    yes
4006                no     no     no
4007                no     no     no
4008                no     no     no
4009                no     no     no
4040                no     no     no
4044                no     no     no
4045                no     no     no
4043                no     no     no
4044                no     no     no
GigabitEthernet6/4 no     no     no
GigabitEthernet6/5 no     no     no
GigabitEthernet6/4 no     no     no
FastEthernet3/4    no     no     no
FastEthernet3/5    no     no     no
GigabitEthernet4/4 no     no     no
GigabitEthernet4/5 no     no     no
GigabitEthernet7/4 no     no     no
GigabitEthernet7/5 no     no     no

Router#
```

Table 2-78 describes the fields that are shown in the example.

**Table 2-78** show mac-address-table learning Field Descriptions

Field	Description
VLAN/Interface <sup>1</sup>	VLAN ID or interface type, module, and port number.
Mod#	Module number of a supervisor engine.
yes	MAC-address learning is enabled.
no	MAC-address learning is disabled.

1. The interfaces displayed are routed interfaces that have internal VLANs assigned to them.

This example shows how to display the status of MAC-address learning on all the existing VLANs on a single supervisor engine:

```
Router# show mac-address-table learning module 4
```

VLAN/Interface	Mod4
4	yes
400	yes
450	yes
500	yes
550	yes
4006	no
4007	no
4008	no
4009	no
4040	no
4044	no
4045	no
4043	no
4044	no
GigabitEthernet6/4	no
GigabitEthernet6/5	no
GigabitEthernet6/4	no
FastEthernet3/4	no
FastEthernet3/5	no
GigabitEthernet4/4	no
GigabitEthernet4/5	no
GigabitEthernet7/4	no
GigabitEthernet7/5	no

```
Router#
```

This example shows how to display the status of MAC-address learning for a specific VLAN on all the supervisor engines:

```
Router# show mac-address-table learning vlan 100
```

VLAN	Mod4	Mod4	Mod7
400	no	no	yes

```
Router
```

This example shows how to display the status of MAC-address learning for a specific VLAN on a specific supervisor engine:

```
Router# show mac-address-table learning vlan 100 module 7
```

VLAN	Mod7
400	yes

```
Router
```

This example shows how to display the status of MAC-address learning for a specific supervisor engine:

```
Router# show mac-address-table learning interface FastEthernet 3/4
```

```
Interface      Mod4    Mod4    Mod7
-----
Fa3/4          no      yes     no
Router
```

This example shows how to display the status of MAC-address learning for a specific interface on a specific supervisor engine:

```
Router# show mac-address-table learning interface FastEthernet 3/4 module 1
```

```
Interface      Mod4
-----
Fa3/4          no
Router
```

#### Related Commands

Command	Description
<a href="#">mac-address-table learning</a>	Enables MAC-address learning.

# show memory dead

To display statistics of memory allocated by processes that are now terminated, use the **show memory dead** command.

**show memory dead [totals]**

## Syntax Description

**totals** (Optional) Displays memory totals for processes that have been terminated.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

The **show memory dead** command displays information about processes that have been terminated. Terminated processes accounts for memory allocated under another process.

## Examples

This example shows the sample output from the **show memory dead** command:

```
Router# show memory dead

      Head   Total (b)   Used (b)   Free (b)   Lowest (b)   Largest (b)
  I/O 600000   5097455   464054   4636458   4635554     4635960

      Processor memory

  Address Bytes Prev1  Next  Ref PrevF NextF Alloc PC What
4D8340   60 4D85C8 4D8378 4
5CA964   36 5CA944 5CA9B4 4          3584FFE Router Init
5CAA04  445 5CA9B4 5CAAA0 4          3A45444 OSPF Stub LSA RBTree
5CAAA0   68 5CAA04 5CAB40 4          3A450D4 Router Init
5ED744   55 5ED668 5ED774 4          3384C84 Router Init
5F45AC   44 5F454C 5F4304 4          3A50534 Router Init
5F4304   54 5F45AC 5F4348 4          3A450D4 Router Init
5F4348   68 5F4304 5F43B8 4          3384C84 Router Init
300C58  340 300A44 300DA8 4          3384B45 Router Init
```

[Table 2-79](#) describes the significant fields shown in the display.

**Table 2-79 show memory dead Field Descriptions**

Field	Description
Head	Hexadecimal address of the head of the memory allocation chain.
Total(b)	Sum of used bytes plus free bytes.
Used(b)	Amount of memory in use.

*Table 2-79 show memory dead Field Descriptions (continued)*

Field	Description
Free(b)	Amount of memory not in use (in bytes).
Lowest(b)	Smallest amount of free memory since last boot (in bytes).
Largest(b)	Size of the largest available free block (in bytes).
Address	Hexadecimal address of the block (in bytes).
Bytes	Size of the block (in bytes).
Prev.	Address of the preceding block.
Next	Address of the following block.
Ref	Reference count for that memory block, indicating how many different processes are using that block of memory.
PrevF	Address of the preceding free block (if free).
NextF	Address of the following free block (if free).
Alloc PC	Address of the system call that allocated the block.
What	Name of the process that owns the block, or “(fragment)” if the block is a fragment, or “(coalesced)” if the block was coalesced from adjacent free blocks.

# show mls asic

To display the ASIC version, use the **show mls asic** command.

**show mls asic**

---

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

---

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

---

**Command Modes** EXEC

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Examples** This example shows how to display the ASIC versions:

```
Router# show mls asic
Earl in Module 5
  Tycho - ver:4 Cisco-id:4C8 Vendor-id:49
Router#
```

## show mls cef

To display the MLS-hardware Layer 3-switching table entries, use the **show mls cef** command.

```
show mls cef [ip] [prefix [mask-length | load-info]] [detail] [module number]
```

```
show mls cef [ip] [{lookup ...} | {multicast ...} | {rpf ...} | {vpn ...} | {vrf ...}]
```

```
show mls cef [{adjacency ...} | {block block-number [entries]} | {config-register reg-address} |
  {diags [detail]} | {entry index [detail]} | {exact-route ...} | {hardware [module number]} |
  {inconsistency ...} | {lookup ...} | {masks [type] [module number]} | {rpf ...} | {statistics ...}
  | {summary [module number]} | {tunnel fragment} | {used-blocks [type] [module number]}
  | {vpn ...} | {vrf ...}]
```

```
show mls cef [{eom ...} | {ip ...} | {ipv6 ...} | {mpls ...}]
```

Syntax	Description
<b>ip</b>	(Optional) Displays IPv6 unicast entries in the MLS-hardware Layer 3-switching table; see the “Usage Guidelines” section for additional information.
<i>prefix</i>	(Optional) Entry prefix in the format A.B.C.D.
<i>mask-length</i>	(Optional) Mask length; valid values are from 0 to 32.
<b>load-info</b>	(Optional) Displays output with a hash value next to each adjacency.
<b>detail</b>	(Optional) Displays detailed hardware information. See the “Usage Guidelines” section for important information.
<b>module number</b>	(Optional) Displays information about the entries for a specific module.
<b>lookup ...</b>	(Optional) Displays IP entries in the MLS-hardware Layer 3-switching table for the specified destination IP address. See the <a href="#">show mls cef lookup</a> command.
<b>multicast ...</b>	(Optional) Displays IP entries in the MLS-hardware Layer 3-switching table in the compact CEF table display format; see the <a href="#">show mls cef ip multicast</a> command.
<b>rpf ...</b>	(Optional) Displays information about the RPF hardware in the MLS-hardware Layer 3-switching table; see the <a href="#">show mls cef rpf</a> command.
<b>vpn ...</b>	(Optional) Displays information about the VPN ID CEF table. See the “Usage Guidelines” section for important information.
<b>vrf ...</b>	(Optional) Displays information about the CEF table for the specified VRF name.
<b>adjacency ...</b>	(Optional) Displays information about the MLS-hardware Layer 3-switching adjacency node; see the <a href="#">show mls cef adjacency</a> command.
<b>block block-number</b>	(Optional) Displays information about the mask-block utilization for a specific block; valid values are from 0 to 4294967295. See the “Usage Guidelines” section for important information.
<b>entries</b>	(Optional) Displays the mask-block utilization entries. See the “Usage Guidelines” section for important information.
<b>config-register reg-address</b>	(Optional) Displays information about the hardware configuration register for a specific register. See the “Usage Guidelines” section for important information.
<b>diags</b>	(Optional) Displays information about the diagnostic entry. See the “Usage Guidelines” section for important information.

<b>entry index</b>	(Optional) Specifies the specified prefix entry index to display; valid values are from 0 to 4294967295. See the “Usage Guidelines” section for important information.
<b>exact-route ...</b>	(Optional) Displays information about hardware load sharing; see the <a href="#">show mls cef exact-route</a> command.
<b>hardware</b>	(Optional) Displays a summary of the hardware information. See the “Usage Guidelines” section for important information.
<b>inconsistency ...</b>	(Optional) Displays information about the consistency checker; see the <a href="#">show mls cef inconsistency</a> command.
<b>masks ...</b>	(Optional) Displays information about the mask. See the “Usage Guidelines” section for important information.
<b>statistics ...</b>	(Optional) Displays the number of switched packets and bytes; see the <a href="#">show mls cef statistics</a> command.
<b>tunnel fragment</b>	(Optional) Displays the operational status of tunnel fragmentation.
<b>summary ...</b>	(Optional) Displays a summary of rates in the hardware for each protocol; see the <a href="#">show mls cef summary</a> command.
<b>used-blocks</b>	(Optional) Displays a list of used blocks; see the “Usage Guidelines” section for important information.
<b>eom ...</b>	Displays information about the EoM protocol; this keyword is not supported.
<b>ip ...</b>	Displays information about the IP protocol; see the “Usage Guidelines” section for additional information.
<b>ipv6 ...</b>	Displays information about the IPv6 protocol.
<b>mpls ...</b>	Displays information about MPLS; see the <a href="#">show mls cef mpls</a> command.

**Defaults**

If you do not specify a protocol, the default display is for IP and the global CEF table.

**Command Modes**

EXEC

**Command History**

Release	Modification
12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

The ... indicates that there is additional information.

The following options are for expert users only and are not documented:

- **load-info**
- **detail**
- **block** *block-number* [**entries**]
- **config-register** *reg-address* }
- **diags** [**detail**]
- **entry** *index* [**detail**]
- **hardware** [**module** *number*]
- **masks** [*type*]
- **used-blocks** [*type*]
- **vpn**

The MLS-hardware Layer 3 switching applies to IP traffic only.

Use the **show mls cef [ip] vrf** command to display the VRF CEF table entries.

You can enter this command on the supervisor engine or switch consoles. Enter the [remote login](#) command to session into the supervisor engine to enter the commands.

The **show mls cef** command offers three levels of options as follows:

- Protocol-independent options—The following keywords are not protocol specific:
  - **adjacency**
  - **exact-route**
  - **inconsistency**
  - **module**
  - **rpf**
  - **statistics**
  - **summary**
  - **used-blocks**
  - **vpn**
  - **vrf**
- Protocol-dependent keywords—The following keywords specify a protocol:
  - **eom**
  - **ip**
  - **ipv6**
  - **mpls**
- Default keywords—The following keywords display identical output for both the **show mls cef** and **show mls cef ip** commands:
  - *prefix*
  - **lookup**

- **multicast**—This keyword is not supported on systems configured with a Supervisor Engine 720.
- **module**
- **rpf**
- **vpn**
- **vrf**

## Examples

This example shows how the **show mls cef** and **show mls cef ip** commands are identical:

```
Router# show mls cef

Codes: decap - Decapsulation, + - Push Label
Index Prefix Adjacency
64 4571010154/35 punt
65 457101010/35 punt
66 457155515551555/35 punt
67 414141400/35 punt
68 4141410/35 punt
69 414141555/35 punt
70 515151400/35 punt
74 5151510/35 punt
75 515151555/35 punt
73 5151515/35 Gi5/5, 00001c00510505
74 0101010/35 punt
75 555155515551555/35 punt
76 50014155155/35 punt
77 500101010/35 punt
78 500155515551555/35 punt
79 50014141453/35 V130, 00501808b18500
84 5001414194/35 V130, 000414eef18800
85 50014141400/35 V130, 00d01bb0510400
83 500145155313/35 V130, 00d01064b17000
84 500151513/35 V130, 00d01064d1500a
85 50014141404/35 V130, 00071ecfc1e40a
86 50010140014/35 V130, 005015a8d1700a
87 50014141404/35 V130, 005010f5d1ac00
88 553155515541556/35 V130, 005015a8d1700a
89 5151517/35 Gi5/5, 00001c00510507
90 4141415/35 Gi5/4, 00001040410405
3500 554101010/54 punt
3504 4141410/54 punt
3505 5151510/54 punt
434400 500101010/8 punt
434435 0101010/0 drop
554556 0101010/0 drop
Router#
```

This example shows how to display all the MLS-hardware Layer 3-switching table IP entries:

```
Router# show mls cef ip

Codes: decap - Decapsulation, + - Push Label
Index Prefix Adjacency
64 4571010154/35 punt
65 457101010/35 punt
66 457155515551555/35 punt
67 414141400/35 punt
68 4141410/35 punt
69 414141555/35 punt
```

```

70      515151400/35      punt
74      5151510/35       punt
75      515151555/35     punt
73      5151515/35       Gi5/5,      00001c00510505
74      0101010/35       punt
75      555155515551555/35 punt
76      50014155155/35   punt
77      500101010/35     punt
78      500155515551555/35 punt
79      50014141453/35   V130,      00501808b18500
84      5001414194/35    V130,      000414eef18800
85      50014141400/35   V130,      00d01bb0510400
83      500145155313/35  V130,      00d01064b17000
84      500151513/35     V130,      00d01064d1500a
85      50014141404/35   V130,      00071ecfc1e40a
86      50010140014/35   V130,      005015a8d1700a
87      50014141404/35   V130,      005010f5d1ac00
88      553155515541556/35 V130,      005015a8d1700a
89      5151517/35       Gi5/5,      00001c00510507
90      4141415/35       Gi5/4,      00001040410405
3500   554101010/54        punt
3504   4141410/54         punt
3505   5151510/54         punt
434400 500101010/8          punt
434435 0101010/0           drop
554556 0101010/0           drop
Router#

```

Table 2-80 describes the fields in the examples.

**Table 2-80** *show mls cef Command Output Fields*

Field	Description
Index	MLS-hardware Layer 3-switching table entry index; the maximum is 256,000 entries.
Prefix	Entry prefix address/mask.
Adjacency	Adjacency types are as follows: <ul style="list-style-type: none"> <li>• drop—Packets matching the prefix entry are dropped.</li> <li>• punt—Packets are redirected to an PISA for further processing.</li> <li>• <i>mac-address</i>—Packets matching the prefix are forwarded to this specific next hop or the final destination host if directly attached.</li> </ul>

This example shows how to display the operational status of tunnel fragmentation:

```

Router# show mls cef tunnel fragment
Tunnel Fragmentation:      Enabled
Router#

```

#### Related Commands

Command	Description
<a href="#">show mls cef summary</a>	Displays the number of routes in the MLS-hardware Layer 3-switching table for all the protocols.

## show mls cef adjacency

To display information about the MLS-hardware Layer 3-switching adjacency node, use the **show mls cef adjacency** command.

```
show mls cef adjacency [all | decap-tunnel | {encap-tunnel ip-src-addr} | {entry index [to
end-range]} | {flags lower-flag upper-flag} | mac-address number | mac-rewrite | macv4 |
{mpls [label]} | multicast | nat | recirculation | special | tcp | usage] [detail] [module number]
```

Syntax Description		
<b>all</b>	(Optional)	Displays all application-allocated entries.
<b>decap-tunnel</b>	(Optional)	Displays the decapsulated tunneled-packet information.
<b>encap-tunnel</b> <i>ip-src-addr</i>	(Optional)	Displays the encapsulated tunnel-adjacency entry that matches the specified address.
<b>entry index</b>	(Optional)	Displays the adjacency-entry information for the specified index; valid values are from 0 to 1048575.
<b>to</b> <i>end-range</i>	(Optional)	Specifies the index range to display adjacency-entry information; valid values are from 0 to 1048575.
<b>flags</b>	(Optional)	Displays information about the specified bit flags. See the “Usage Guidelines” section for additional information.
<i>lower-flag</i>		Lower 32-bits flag values to display; valid values are 0 to FFFFFFFF.
<i>upper-flag</i>		Upper 32-bits flag values to display; valid values are 0 to FFFFFFFF.
<b>mac-address</b> <i>number</i>	(Optional)	Displays information about the matched MAC-address adjacency for the specified 48-bit hardware address in the H.H.H format.
<b>mac-rewrite</b>	(Optional)	Displays information about the MAC-rewrite adjacency.
<b>macv4</b>	(Optional)	Displays information about the MACv4 adjacency.
<b>mpls</b>	(Optional)	Displays information about the MPLS adjacency.
<i>label</i>	(Optional)	MPLS label to display adjacency-entry information; valid values are from 0 to 1048575.
<b>multicast</b>	(Optional)	Displays information about the multicast adjacency.
<b>nat</b>	(Optional)	Displays information about the NAT adjacency.
<b>recirculation</b>	(Optional)	Displays information about the recirculated-adjacency entry.
<b>special</b>	(Optional)	Displays information about the special adjacencies.
<b>tcp</b>	(Optional)	Displays information about the TCP-application adjacency.
<b>usage</b>	(Optional)	Displays information about the adjacency usage.
<b>detail</b>	(Optional)	Displays hardware-entry details.
<b>module</b> <i>number</i>	(Optional)	Displays information about the adjacency node for a specific module.

### Defaults

This command has no default settings.

### Command Modes

EXEC

**Command History**

Release	Modification
12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

The **decap-tunnel** and **encap-tunnel** keywords are used to display the tunnel nodes. The encapsulator node is considered the tunnel-entry point and the decapsulator node is considered the tunnel-exit point. There may be multiple source-destination pairs using the same tunnel between the encapsulator and decapsulator.

The **decap-tunnel** and **encap-tunnel** keywords are not supported on Catalyst 6500 series switches that are configured with a Supervisor Engine 720.

The **flags** keyword applies to all adjacency formats (for example, mac-rewrite, mpls, and multicast) and indicates the bits that are set in the adjacency for the specific adjacency.

The **module number** keyword and argument designate the module and port number. Valid values depend on the chassis and module used. For example, if you have a 48-port 10/100BASE-T Ethernet module installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

MLS-hardware Layer 3 switching applies to IP traffic only.

MLS-hardware Layer 3-switching adjacency statistics are updated every 60 seconds.

You can display hardware-switched IP-directed broadcast information by entering the **show mls cef adjacency mac-address number detail** command.

For each MLS-hardware Layer 3-switching FIB entry, MLS-hardware Layer 3 switching stores Layer 2 information from the PISA for adjacent nodes in the MLS-hardware Layer 3-switching adjacency table. Adjacent nodes are directly connected at Layer 2. To forward traffic, MLS-hardware Layer 3 switching selects a route from a MLS-hardware Layer 3-switching FIB entry, which points to a MLS-hardware Layer 3-switching adjacency entry, and uses the Layer 2 header for the adjacent node in the adjacency table entry to rewrite the packet during Layer 3 switching. MLS-hardware Layer 3 switching supports one million adjacency-table entries.

**Examples**

This example shows how to display information for all adjacency nodes:

```
Router# show mls cef adjacency all

Index: 5      smac: 00001000010000, dmac: 00001000010000
             mtu: 0, vlan: 0, dindex: 0x0, l3rw_vld: 0
             packets: 0, bytes: 0

Index: 35773  smac: 00001000010000, dmac: 00001000010000
             mtu: 0, vlan: 0, dindex: 0x0, l3rw_vld: 0
             packets: 0, bytes: 0
<Output is truncated>
```

This example shows how to display the adjacency-entry information for a specific index:

```
Router# show mls cef adjacency entry 132

Index: 435      smac: 00001000010000, dmac: 00001000010000
                mtu: 0, vlan: 0, dindex: 0x0, l3rw_vld: 0
                packets: 0, bytes: 0
```

This example shows how to display the adjacency-entry information for a range of indexes:

```
Router# show mls cef adjacency entry 132 to 134

Index: 435      smac: 00001000010000, dmac: 00001000010000
                mtu: 0, vlan: 0, dindex: 0x0, l3rw_vld: 0
                packets: 0, bytes: 0

Index: 433      smac: 00001000010000, dmac: 00001000010000
                mtu: 0, vlan: 0, dindex: 0x0, l3rw_vld: 0
                packets: 0, bytes: 0

Index: 434      smac: 00001000010000, dmac: 00001000010000
                mtu: 0, vlan: 0, dindex: 0x0, l3rw_vld: 0
                packets: 0, bytes: 0

Router#
```

This example shows how to display recirculation-adjacency information:

```
Router# show mls cef adjacency recirculation detail
Index: 6        smac: 00001000010000, dmac: 00001000010000
                mtu: 65535, vlan: 0, dindex: 0x0, ccc = 440,
                format: RECIR, l3rw_vld: 4

Router#
```

This example shows how to display specific bit flags:

```
Router# show mls cef adjacency flags 8408 0

STAT_REQUIRED NO_STAT CAP4 IQO UTTL UTOS
Router#
```

This example shows how to display adjacency-node information for a specific MAC address:

```
Router# show mls cef adjacency mac-address 00e0.f74c.842d

Index: 433438  smac: 00d01064d1500a, dmac: 00e01f74c1845d
                mtu: 4548, vlan: 45, dindex: 0x0, l3rw_vld: 4
                packets: 0, bytes: 0

Index: 433444  smac: 00d01064d1500a, dmac: 00e01f74c1845d
                mtu: 4548, vlan: 45, dindex: 0x0, l3rw_vld: 4
                packets: 0, bytes: 0

Router#
```

This example shows how to display the MAC-rewrite adjacency information:

```
Router# show mls cef adjacency mac-rewrite

Index: 433435  smac: 00001000010000, dmac: 00001000010000
                mtu: 0, vlan: 0, dindex: 0x0, l3rw_vld: 0
                packets: 0, bytes: 0

Index: 433433  smac: 000a1454f13000, dmac: 005015a8d1700a
                mtu: 4548, vlan: 4, dindex: 0x0, l3rw_vld: 4
                packets: 0, bytes: 0
```

```
Index: 433434 smac: 000a1454f13000, dmac: 00001750410004
          mtu: 4548, vlan: 75, dindex: 0x0, l3rw_vld: 4
          packets: 0, bytes: 0
```

```
Index: 433435 smac: 000a1454f13000, dmac: 00001730410004
          mtu: 4548, vlan: 73, dindex: 0x0, l3rw_vld: 4
          packets: 0, bytes: 0
```

<Output is truncated>

This example shows how to display information about the MPLS adjacency:

```
Router# show mls cef adjacency mpls detail
Index: 35768 smac: 00001000010000, dmac: 00001000010000
mtu: 4544, vlan: 0, dindex: 0x7FFA, l3rw_vld: 4
format: MPLS, flags: 0x4000408600
label0: 0, exp: 0, ovr: 0
label4: 0, exp: 0, ovr: 0
label5: 0, exp: 0, ovr: 0
op: POP
packets: 0, bytes: 0
Router#
```

This example shows how to display information about the multicast adjacency:

```
Router# show mls cef adjacency multicast detail
Index: 55 smac: 00001000010000, dmac: 00001000010000
mtu: 0, vlan: 0, dindex: 0x0, l3rw_vld: 0
format: MULTICAST, flags: 0x800
met5: 0, met3: 0
packets: 5535, bytes: 480684
Router#
```

This example shows how to display information about the NAT adjacency:

```
Router# show mls cef adjacency nat detail
Index: 500 mtu: 4555, vlan: 4063, dindex: 0x7FFA, l3rw_vld: 4
format: NAT, flags: 0x8600
ip_sa: 5151515, src_port: 400
ip_da: 3131313, dst_port: 300
delta_seq: 0, delta_ack: 0
packets: 0, bytes: 0
Router#
```

This example shows how to display information about the special adjacency:

```
Router# show mls cef adjacency special

Index: 0          smac: 00001000010000, dmac: 00001000010000
                  mtu: 9534, vlan: 0, dindex: 0x0, l3rw_vld: 0
                  format: MULTICAST, flags: 0x800 (mcast_fib_fail)
                  met5: 0, met3: 0
                  packets: 0, bytes: 0

Index: 4          smac: 00001000010000, dmac: 00001000010000
                  mtu: 9534, vlan: 0, dindex: 0x0, l3rw_vld: 0
                  format: MULTICAST, flags: 0x800 (mcast_fib_rf_cr)
                  met5: 0, met3: 0
                  packets: 0, bytes: 0
```

<Output is truncated>

This example shows how to display information about the TCP adjacency:

```
Router# show mls cef adjacency tcp detail
Index: 500 smac: abcd1abcd1abcd, dmac: 00001400015000
mtu: 4548, vlan: 4063, dindex: 0x0, l3rw_vld: 4
format: MAC_TCP, flags: 0x8408
delta_seq: 40, delta_ack: 0
packets: 0, bytes: 0
Router#
```

This example shows how to display information about the adjacency usage:

```
Router# show mls cef adjacency usage

Adjacency Table Size: 4048576
ACL region usage: 5
Non-stats region usage: 458
Stats region usage: 34
Total adjacency usage: 464
Router#
```

# show mls cef exact-route

To display information about the hardware load sharing, use the **show mls cef exact-route** command.

```
show mls cef exact-route src-ip {dest-ip | src-l4port} [dest-l4port | {module num}]
```

```
show mls cef exact-route {vrf instance-name} src-ip {dest-ip | src-l4port} [dest-l4port | {module num}]
```

Syntax Description		
<i>src-ip</i>	Source IP address.	
<i>dest-ip</i>	Destination IP address.	
<i>src-l4port</i>	Layer 4-source port number; valid values are from 0 to 65535.	
<i>dest-l4port</i>	(Optional) Layer 4-destination port number; valid values are from 0 to 65535.	
<b>module num</b>	(Optional) Module number.	
<b>vrf</b> <i>instance-name</i>	Displays the numeric VPN routing and forwarding ID for the specified VRF instance name.	

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **vrf** *instance-name* keyword and argument are not supported on Catalyst 6500 series switches that are configured with a Supervisor Engine 2.

**Examples** This example shows how to display the hardware load-sharing information:

```
Router# show mls cef exact-route 172.20.52.16 172.20.52.31
```

```
Interface: Gi5/4, Next Hop: 555155515551555, Vlan: 4073, Destination Mac: 00d01064d1500a
```

```
Router#
```

Related Commands	Command	Description
	<b>show ip cef exact-route</b>	Displays the exact route for a source-destination IP address pair.

# show mls cef exception

To display information about the CEF exception, use the **show mls cef exception** command.

```
show mls cef exception {status [detail] | priorities}
```

Syntax Description	status	Displays information about the CEF-exception status.
	detail	(Optional) Displays detailed hardware information; see the “Usage Guidelines” section for more information.
	priorities	Displays information about the CEF-exception priority.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **detail** keyword is for expert users only and is not documented. In the output of the **show mls cef exception status** command, the following definitions apply:

- FALSE—Indicates that the protocol is not under the exception.
- TRUE—Indicates that the protocol is under the exception.

**Examples** This example shows how to display detailed information about the CEF-exception status:

```
Router# show mls cef exception status
Current IPv4 FIB exception state = FALSE
Current IPv6 FIB exception state = FALSE
Current MPLS FIB exception state = FALSE
Router#
```

This example shows how to display the FIB ERM-exception priority:

```
Router# show mls cef exception priorities
Priority Protocol
=====
4 IPv4
5 IPv6
3 MPLS
Router#
```

---

**Related Commands**

Command	Description
<a href="#">mls erm priority</a>	Assigns the priorities to define an order in which protocols attempt to recover from the exception status.

---

## show mls cef hardware

To display the MLS-hardware Layer 3-switching table entries, use the **show mls cef hardware** command.

**show mls cef hardware** [*module number*]

<b>Syntax Description</b>	<b>module number</b> (Optional) Displays the adjacency-node information for a specific module.
---------------------------	--

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	MLS-hardware Layer 3 switching applies to IP traffic only.
-------------------------	--

<b>Examples</b>	This example shows how to display all the MLS-hardware Layer 3-switching table entries:
-----------------	---

```
Router# show mls cef hardware

CEF TCAM v5:
Size:
  65536 rows/device, 4 device(s), 565444 total rows
  35 entries/mask-block
  8495 total blocks (35b wide)
  4545446 s/w table memory
Options:
  sanity check: on
  sanity interval: 304 seconds
  consistency check: on
  consistency interval: 64 seconds
  redistribution: off
    redistribution interval: 450 seconds
    redistribution threshold: 40
  compression: on
    compression interval: 34 seconds
  tcam/ssram shadowing: on
Operation Statistics:
  Entries inserted:          0000000000000054
  Entries deleted:          0000000000000005
  Entries compressed:       0000000000000000
  Blocks inserted:          0000000000000048
  Blocks deleted:           0000000000000004
  Blocks compressed:        0000000000000000
  Blocks shuffled:          0000000000000005
  Blocks deleted for exception: 0000000000000000
```

```

Direct h/w modifications:          0000000000000000

Background Task Statistics:
Consistency Check count:          0000000000044066
Consistency Errors:                0000000000000000
SSRAM Consistency Errors:         0000000000000000
Sanity Check count:               000000000005855
Sanity Check Errors:              0000000000000000
Compression count:                000000000004654

Exception Handling status   : on
L3 Hardware switching status : on
Fatal Error Handling Status : Reset
Fatal Errors:               0000000000000000
Fatal Error Recovery Count: 0000000000000000

SSRAM ECC error summary:
Uncorrectable ecc entries   : 0
Correctable ecc entries    : 0
Packets dropped             : 0
Packets software switched  : 0

FIB SSRAM Entry status
-----
Key: UC - Uncorrectable error, C - Correctable error
     SSRAM banks : Bank0   Bank4
No ECC errors reported in FIB SSRAM1

```

# show mls cef inconsistency

To display consistency-checker information, use the **show mls cef inconsistency** command.

```
show mls cef inconsistency [module num | now | records] [detail] [module num]
```

Syntax Description	Parameter	Description
	<b>module num</b>	(Optional) Displays inconsistency information for the specified module.
	<b>now</b>	(Optional) Runs a consistency check and displays any issues.
	<b>records</b>	(Optional) Displays the inconsistency records.
	<b>detail</b>	(Optional) Displays hardware-entry details.
	<b>module num</b>	(Optional) Displays the adjacency-node information for a specific module.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** If you enter the **show mls cef inconsistency** command with no arguments, this information is displayed:

- Consistency check count
- TCAM-consistency check errors
- SSRAM-consistency check errors

**Examples** This example shows how to display information about the consistency checker:

```
Router# show mls cef inconsistency
Consistency Check Count      : 84
TCAM Consistency Check Errors : 0
SSRAM Consistency Check Errors : 0
Router#
```

This example shows how to display information about the consistency checker for a specific module:

```
Router# show mls cef inconsistency module 7
Consistency Check Count      : 44033
TCAM Consistency Check Errors : 0
SSRAM Consistency Check Errors : 0
Router#
```

This example shows how to run a consistency check and display any issues:

```
Router# show mls cef inconsistency now
Performing TCAM check now l1ldone
No1 of FIB TCAM Consistency Check Errors : 0
Performing SSRAM check now l1ldone
No1 of FIB SSRAM Consistency Check Errors : 0
```

Router#

This example shows how to display the consistency records:

```
Router# show mls cef inconsistency records
Consistency Check Count      : 44044
TCAM Consistency Check Errors : 0
SSRAM Consistency Check Errors : 0
```

Router#

# show mls cef ip

To display the IP entries in the MLS-hardware Layer 3-switching table, use the **show mls cef ip** command.

```
show mls cef ip [prefix [mask-length]] [detail] [module number]
```

```
show mls cef ip accounting per-prefix
```

```
show mls cef ip {lookup ...} | {multicast team ...} | {rpf ...} | {vpn ...} | {vrf ...}
```

Syntax Description		
<i>prefix</i>	(Optional) Entry prefix in the format A.B.C.D.	
<i>mask-length</i>	(Optional) Mask length; valid values are from 0 to 32.	
<b>detail</b>	(Optional) Displays hardware-entry details.	
<b>module number</b>	(Optional) Displays the entries for a specific module.	
<b>accounting per-prefix</b>	Displays all the prefixes that are configured for the statistic collection.	
<b>lookup ...</b>	Displays the TCAM-entry index for the specified destination IP unicast address; see the <a href="#">show mls cef lookup</a> command.	
<b>multicast team ...</b>	Displays the IP entries in the MLS-hardware Layer 3-switching table in the compact CEF table-display format; see the “Usage Guidelines” section for additional information.	
<b>rpf ...</b>	Displays the RPF-hardware information in the MLS-hardware Layer 3-switching table; see the <a href="#">show mls cef rpf</a> command.	
<b>vpn ...</b>	(Optional) Displays information about the VPN ID CEF table; see the “Usage Guidelines” section for more information.	
<b>vrf ...</b>	Displays information about the VPN-instance CEF table.	

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** See the [show mls cef ip multicast team](#) command for information about this command.

The ... indicates that there is additional information.

The **vpn** keyword is for expert users only and is not documented.

Information in the output of the **show mls cef ip** command is also displayed in the **show mls cef** commands.

The lookup is performed as a “longest prefix match” and displays the TCAM-entry index that applies to the specified destination IP address.

The information output is in this format: Index, Prefix, Mask, and Adjacency.

### Examples

This example shows how the **show mls cef** and **show mls cef ip** commands are identical:

```
Router# show mls cef

Codes: decap - Decapsulation, + - Push Label
Index Prefix Adjacency
64 4571010154/35 punt
65 457101010/35 punt
66 457155515551555/35 punt
67 414141400/35 punt
68 4141410/35 punt
69 414141555/35 punt
70 515151400/35 punt
74 5151510/35 punt
75 515151555/35 punt
73 5151515/35 Gi5/5, 00001c00510505
74 0101010/35 punt
75 555155515551555/35 punt
76 50014155155/35 punt
77 500101010/35 punt
78 500155515551555/35 punt
79 50014141453/35 Vl30, 00501808b18500
84 5001414194/35 Vl30, 000414eef18800
85 50014141400/35 Vl30, 00d01bb0510400
83 500145155313/35 Vl30, 00d01064b17000
84 500151513/35 Vl30, 00d01064d1500a
85 50014141404/35 Vl30, 00071ecfc1e40a
86 50010140014/35 Vl30, 005015a8d1700a
87 50014141404/35 Vl30, 005010f5d1ac00
88 553155515541556/35 Vl30, 005015a8d1700a
89 5151517/35 Gi5/5, 00001c00510507
90 4141415/35 Gi5/4, 00001040410405
3500 554101010/54 punt
3504 4141410/54 punt
3505 5151510/54 punt
434400 500101010/8 punt
434435 0101010/0 drop
554556 0101010/0 drop
Router#
```

This example shows how to display all the MLS-hardware Layer 3-switching table IP entries:

```
Router# show mls cef ip

Codes: decap - Decapsulation, + - Push Label
Index  Prefix                Adjacency
64     4571010154/35          punt
65     457101010/35           punt
66     457155515551555/35    punt
67     414141400/35          punt
68     4141410/35            punt
69     414141555/35          punt
70     515151400/35          punt
74     5151510/35            punt
75     515151555/35          punt
73     5151515/35            Gi5/5,          00001c00510505
74     0101010/35            punt
75     555155515551555/35    punt
76     50014155155/35        punt
77     500101010/35          punt
78     500155515551555/35    punt
79     50014141453/35        V130,          00501808b18500
84     5001414194/35         V130           000414eef18800
85     50014141400/35        V130           00d01bb0510400
83     500145155313/35       V130           00d01064b17000
84     500151513/35          V130           00d01064d1500a
85     50014141404/35        V130           00071ecfc1e40a
86     50010140014/35        V130           005015a8d1700a
87     50014141404/35        V130           005010f5d1ac00
88     553155515541556/35    V130           005015a8d1700a
89     5151517/35            Gi5/5          00001c00510507
90     4141415/35            Gi5/4          00001040410405
3500   554101010/54          punt
3504   4141410/54            punt
3505   5151510/54            punt
434400 500101010/8           punt
434435 0101010/0             drop
554556 0101010/0             drop
Router#
```

Table 2-81 describes the fields shown in the examples.

**Table 2-81 show mls cef ip Command Output Fields**

Field	Description
Index	MLS-hardware Layer 3-switching table entry index; the maximum is 256,000 entries.
Prefix	Entry prefix address/mask.
Adjacency	Adjacency information.

This example shows how to display the detailed MLS-hardware Layer 3-switching table entries:

```
Router# show mls cef ip 127.0.0.52 detail

Codes: M - mask entry, V - value entry, A - adjacency index, P - priority bit
       D - full don't switch, m - load balancing modnumber, B - BGP Bucket sel
       V0 - Vlan 0,C0 - don't comp bit 0,V4 - Vlan 4,C4 - don't comp bit 4
       RVTEN - RPF Vlan table enable, RVTSEL - RPF Vlan table select
```

```

Format: IPV4_DA - (8 ; xtag vpn pi cr recirc tos prefix)
Format: IPV4_SA - (9 ; xtag vpn pi cr recirc prefix)
M(494  ): E ; 4 FFF 0 0 0 0 555155515551555
V(494  ): 8 ; 4 0 0 0 0 4571010155 (A:433450 ,P:4,D:0,m:0 ,B:0)
Router#

```

This example shows how to display all the prefixes that are configured for the statistic collection:

```

Router# show mls cef ip accounting per-prefix
      VRF          Prefix/Mask          Packets          Bytes

A - Active, I - Inactive
Router#

```

#### Related Commands

Command	Description
<a href="#">show mls cef</a>	Displays the MLS-hardware Layer 3-switching table entries.

## show mls cef ip multicast

To display the IP entries in the multilayer switching (MLS)-hardware Layer 3-switching table on the switch processor, use the **show mls cef ip multicast** command.

```
show mls cef ip multicast { bidir | grp-only | source source-ip } [detail | group group-id |
  vlan rpf-vlanid]
```

```
show mls cef ip multicast control [detail | prefix prefix | vlan rpf-vlanid]
```

```
show mls cef ip multicast group group-id [detail | vlan rpf-vlanid]
```

```
show mls cef ip multicast src-grp [detail | group group-ip | source | vlan rpf-vlanid]
```

```
show mls cef ip multicast subnet [detail | prefix prefix | vlan rpf-vlanid]
```

```
show mls cef ip multicast summary [vpn-num]
```

```
show mls cef ip multicast tcam [prefix [mask]] [detail] [module num] [vrf src-ip {src-port |
  dst-ip} [dst-port | module num]]
```

```
show mls cef ip multicast { grp-mask | vlan rpf-vlanid / vpn vpn-id } [detail]
```

### Syntax Description

<b>bidir</b>	Displays Bidir information.
<b>grp-only</b>	Displays hardware-entry information that is based on (*,G) shortcuts; see the “Usage Guidelines” section for additional information.
<b>source</b> <i>source-ip</i>	Displays hardware-entry information based on the specified source IP address.
<b>detail</b>	(Optional) Displays hardware-entry details.
<b>group</b> <i>group-id</i>	(Optional) Displays hardware-entry information that is based on the specified group IP address.
<b>vlan</b> <i>rpf-vlanid</i>	(Optional) Displays information for a specific RPF VLAN ID; valid values are from 0 to 4095.
<b>control</b>	(Optional) Displays hardware-entry information that is based on (*,G/m) entries; see the “Usage Guidelines” section for additional information.
<b>prefix</b> <i>prefix</i>	(Optional) Displays hardware-entry information that is based on an IP subnet prefix.
<b>src-grp</b>	Displays hardware-entry information that is based on (S,G) shortcuts; see the “Usage Guidelines” section for additional information.
<b>subnet</b>	Displays hardware-entry information that is based on (S/m,*) shortcuts; see the “Usage Guidelines” section for additional information.
<b>summary</b>	Displays a summary of installed-hardware shortcuts.
<b>tcam</b>	Displays CEF-table information in a compact format; see the “Usage Guidelines” section for additional information.
<b>mask</b>	(Optional) Displays hardware-entry information that is based on the specified subnet mask.
<b>vrf</b> <i>src-ip</i>	(Optional) Displays the numeric VRF ID for the specified source IP address.
<i>src-port</i>	(Optional) Layer 4 source port; valid values are from 0 to 65535.
<i>dst-ip</i>	(Optional) Destination IP address.

<i>dst-port</i>	(Optional) Layer 4 destination port; valid values are from 0 to 65535.
<b>grp-mask</b>	Displays hardware-entry information that is based on Bidir (*,G/m) shortcuts.
<b>vpn vpn-id</b>	Displays hardware-entry information that is based on the specified VPN ID; valid values are from 0 to 4095.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** There are two MMLS modes, ingress and egress. The output displayed differs for each mode.

The hardware-entry types are as follows:

- {S/m,\*}—Interface/mask (or subnet) entries that are used to catch a directly connected source.
- {\*,G/m}—Groups that are served by the route processors as group/mask.
- {G,C}—G indicates a destination MAC address, which is derived from an IP-multicast address, and C indicates the ingress VLAN.
- {S,G,C}—S indicates the source IP address, G indicates the destination IP address, which is a multicast address, and C indicates the ingress VLAN, which is usually the RPF VLAN of the flow.
- {S,G}—Multicast-routing table entry that is maintained by the software or a multicast-forwarding table entry that is created in the FIB table.
- {\*,G}—Same as {S,G}, except that the source address is a wildcard.

The DF index field ranges from 1 to 4 and is an index into the acceptance (PIM route processors multiplied by the DF) table. The acceptance table is used with DF forwarding and is used to identify the set of DF interfaces for each of the four RPs in a VPN.

**Examples** This example shows how to display ingress hardware-entry information that is based on Bidir (\*,G/m) shortcuts:

```
Router# show mls cef ip multicast grp-mask
```

```
Multicast CEF Entries for VPN#0
Flags: R - Control, S - Subnet, B - Bidir, C - Complete, P - Partial,
       c - Central Rewrite, p - Primary Input, r - Recirculation
Source/mask      Destination/mask    RPF/DF  Flags #packets      #bytes
rwindex  Output Vlans/Info
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
*          556151510/54      Df0    BCp   0         0         -
Vl50 [4 oifs]
*          555151510/54      Df4    BCp   0         0         -
Vl54 [4 oifs]
```

■ **show mls cef ip multicast**

```
*
          557151510/54      Df4   BCp   0           0           -
Vl154 [4 oifs]
Found 3 entries1 3 are mfd entries
Router#
```

This example shows how to display detailed ingress hardware-entry information that is based on Bidir (\*,G/m) shortcuts:

```
Router# show mls cef ip multicast grp-mask detail
(*, 556151510/54)
  PI:4 (4) CR:0 (0) Recirc:0 (4)
  DFidx:0 AdjPtr:7,35775,65543,98344 FibRpfNf:0 FibRpfDf:0 FibAddr:0x400
  rwlans:0 rwindex:0x0 adjmac:00061d6061e540 rdt:0 E:0 CAP4:0
  fmt:mcast 13rwwld:4 DM:0 mtu:4548 rwttype:L3 met5:0x0 met3:0x5
  packets:000000000000 bytes:000000000000000000
  Starting Offset: 0x0005
  V E C:  50 I:0x00449

(*, 555151510/54)
  PI:4 (4) CR:0 (0) Recirc:0 (4)
  DFidx:4 AdjPtr:8,35776,65544,98345 FibRpfNf:0 FibRpfDf:0 FibAddr:0x405
  rwlans:0 rwindex:0x0 adjmac:00061d6061e540 rdt:0 E:0 CAP4:0
  fmt:mcast 13rwwld:4 DM:0 mtu:4548 rwttype:L3 met5:0x0 met3:0x6
  packets:000000000000 bytes:000000000000000000
  Starting Offset: 0x0006
  V E C:  54 I:0x0044B

(*, 557151510/54)
  PI:4 (4) CR:0 (0) Recirc:0 (4)
  DFidx:4 AdjPtr:49,35787,65555,98353 FibRpfNf:0 FibRpfDf:0 FibAddr:0x404
  rwlans:0 rwindex:0x0 adjmac:00061d6061e540 rdt:0 E:0 CAP4:0
  fmt:mcast 13rwwld:4 DM:0 mtu:4548 rwttype:L3 met5:0x0 met3:0x7
  packets:000000000000 bytes:000000000000000000
  Starting Offset: 0x0007
  V E C:  54 I:0x0044B

Found 3 entries1 3 are mfd entries
Router#
```

This example shows how to display ingress-Bidir information:

```
Router# show mls cef ip multicast bidir

Multicast CEF Entries for VPN#0
Flags: R - Control, S - Subnet, B - Bidir, C - Complete, P - Partial,
       c - Central Rewrite, p - Primary Input, r - Recirculation
Source/mask      Destination/mask   RPF/DF  Flags #packets      #bytes
rwindex  Output Vlans/Info
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
-----+-----+-----+-----+-----+-----+-----+-----+-----+
*          555151515/35      Df4   BCp   0           0           -
Vl154,Vl130 [5 oifs]
*          555151514/35      Df4   BCp   0           0           -
Vl154,Vl130 [5 oifs]
Found 5 entries1 5 are mfd entries
Router#
```

This example shows how to display detailed ingress-Bidir information:

```
Router# show mls cef ip multicast bidir detail

(*, 555151515)
  PI:4 (4) CR:0 (0) Recirc:0 (4)
  DFidx:4 AdjPtr:40,35778,65546,98344 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE5
```

```

rwlans:0 rwindex:0x0 adjmac:00061d6061e540 rdt:0 E:0 CAP4:0
fmt:mcast l3rwvld:4 DM:0 mtu:4548 rwtype:L3 met5:0x0 met3:0xA
packets:000000000000 bytes:0000000000000000
Starting Offset: 0x000A
  V C:  54 I:0x004B5 P->49A0
- V
  V E C:  30 I:0x0049B

```

```

(*, 555151514)
  PI:4 (4) CR:0 (0) Recirc:0 (4)
  DFidx:4 AdjPtr:9,35777,65545,98343 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE0
rwlans:0 rwindex:0x0 adjmac:00061d6061e540 rdt:0 E:0 CAP4:0
fmt:mcast l3rwvld:4 DM:0 mtu:4548 rwtype:L3 met5:0x0 met3:0x8
packets:000000000000 bytes:0000000000000000
Starting Offset: 0x0008
  V C:  54 I:0x004B4 P->499C
- V
  V E C:  30 I:0x00499

```

Found 5 entries1 5 are mfd entries  
Router#

This example shows how to display egress hardware-entry information that is based on Bidir (\*,G/m) shortcuts:

Router# **show mls cef ip multicast grp-mask**

```

Multicast CEF Entries for VPN#0
Flags: R - Control, S - Subnet, B - Bidir, C - Complete, P - Partial,
       c - Central Rewrite, p - Primary Input, r - Recirculation
Source/mask      Destination/mask      RPF/DF  Flags #packets      #bytes
rwindex  Output Vlans/Info
+-----+-----+-----+-----+-----+-----+-----+
-----+-----+-----+-----+-----+-----+-----+
*           555151510/54      Df0    BCp  0          0          -
*           555151510/54      -      Bpr  0          0
0x4AE  Vl54 [4 oifs]
*           555151510/54      -      Br   0          0
0x40E  Vl54 [4 oifs]
*           556151510/54      Df4    BCp  0          0          -
*           556151510/54      -      Bpr  0          0
0x4AE  Vl50 [4 oifs]
*           556151510/54      -      Br   0          0
0x40E  Vl50 [4 oifs]
*           557151510/54      Df0    BCp  0          0          -
*           557151510/54      -      Bpr  0          0
0x4AE  Vl54 [4 oifs]
*           557151510/54      -      Br   0          0
0x40E  Vl54 [4 oifs]
Found 3 entries1 3 are mfd entries
Router#

```

This example shows how to display detailed egress hardware-entry information that is based on Bidir (\*,G/m) shortcuts:

```

Router# show mls cef ip multicast grp-mask detail
(*, 555151510/54)
  PI:4 (4) CR:0 (0) Recirc:0 (4)
  DFidx:0 AdjPtr:7,35775,65543,98344 FibRpfNf:0 FibRpfDf:0 FibAddr:0x450
rwlans:0 rwindex:0x0 rdt:0 E:0 CAP4:0
fmt:recir l3rwvld:4 DM:0 mtu:4555 rwtype:RECIR
packets:000000000000 bytes:0000000000000000
  PI:4 (4) CR:0 (0) Recirc:4 (4)

```

```

AdjPtr:8,35776,65544,98345 FibRpfNf:0 FibRpfDf:0 FibAddr:0x455
rwlans:0 rwindex:0x4AE adjmac:00061d6061e540 rdt:4 E:4 CAP4:0
fmt:mcast l3rwlvd:4 DM:0 mtu:4555 rwtype:L3 met5:0x0 met3:0x5
packets:000000000000 bytes:000000000000000000
Starting Offset: 0x0005
V E C: 54 I:0x0044C

```

```

PI:0 (4) CR:0 (0) Recirc:4 (4)
AdjPtr:9,35777,65545,98343 FibRpfNf:0 FibRpfDf:0 FibAddr:0x454
rwlans:0 rwindex:0x40E adjmac:00061d6061e540 rdt:4 E:0 CAP4:0
fmt:mcast l3rwlvd:4 DM:0 mtu:4555 rwtype:L3 met5:0x0 met3:0x5
packets:000000000000 bytes:000000000000000000
Starting Offset: 0x0005
V E C: 54 I:0x0044C

```

```
(* , 556151510/54)
```

```

PI:4 (4) CR:0 (0) Recirc:0 (4)
DFidx:4 AdjPtr:40,35778,65546,98344 FibRpfNf:0 FibRpfDf:0 FibAddr:0x456
rwlans:0 rwindex:0x0 rdt:0 E:0 CAP4:0
fmt:recir l3rwlvd:4 DM:0 mtu:4555 rwtype:RECIR
packets:000000000000 bytes:000000000000000000

```

```

PI:4 (4) CR:0 (0) Recirc:4 (4)
AdjPtr:44,35779,65547,98345 FibRpfNf:0 FibRpfDf:0 FibAddr:0x458
rwlans:0 rwindex:0x4AE adjmac:00061d6061e540 rdt:4 E:4 CAP4:0
fmt:mcast l3rwlvd:4 DM:0 mtu:4555 rwtype:L3 met5:0x0 met3:0x4C
packets:000000000000 bytes:000000000000000000
Starting Offset: 0x004C
V E C: 50 I:0x00447

```

```

PI:0 (4) CR:0 (0) Recirc:4 (4)
AdjPtr:45,35780,65548,98346 FibRpfNf:0 FibRpfDf:0 FibAddr:0x45A
rwlans:0 rwindex:0x40E adjmac:00061d6061e540 rdt:4 E:0 CAP4:0
fmt:mcast l3rwlvd:4 DM:0 mtu:4555 rwtype:L3 met5:0x0 met3:0x4C
packets:000000000000 bytes:000000000000000000
Starting Offset: 0x004C
V E C: 50 I:0x00447

```

```
(* , 557151510/54)
```

```

PI:4 (4) CR:0 (0) Recirc:0 (4)
DFidx:0 AdjPtr:43,35784,65549,98347 FibRpfNf:0 FibRpfDf:0 FibAddr:0x45C
rwlans:0 rwindex:0x0 rdt:0 E:0 CAP4:0
fmt:recir l3rwlvd:4 DM:0 mtu:4555 rwtype:RECIR
packets:000000000000 bytes:000000000000000000

```

```

PI:4 (4) CR:0 (0) Recirc:4 (4)
AdjPtr:44,35785,65550,98348 FibRpfNf:0 FibRpfDf:0 FibAddr:0x45E
rwlans:0 rwindex:0x4AE adjmac:00061d6061e540 rdt:4 E:4 CAP4:0
fmt:mcast l3rwlvd:4 DM:0 mtu:4555 rwtype:L3 met5:0x0 met3:0x4D
packets:000000000000 bytes:000000000000000000
Starting Offset: 0x004D
V E C: 54 I:0x0044C

```

```

PI:0 (4) CR:0 (0) Recirc:4 (4)
AdjPtr:45,35783,65554,98349 FibRpfNf:0 FibRpfDf:0 FibAddr:0x430
rwlans:0 rwindex:0x40E adjmac:00061d6061e540 rdt:4 E:0 CAP4:0
fmt:mcast l3rwlvd:4 DM:0 mtu:4555 rwtype:L3 met5:0x0 met3:0x4D
packets:000000000000 bytes:000000000000000000
Starting Offset: 0x004D
V E C: 54 I:0x0044C

```

```

Found 3 entries1 3 are mfd entries
Router#

```

This example shows how to display egress-Bidir information:

```
Router# show mls cef ip multicast bidir
```

```
Multicast CEF Entries for VPN#0
Flags: R - Control, S - Subnet, B - Bidir, C - Complete, P - Partial,
      c - Central Rewrite, p - Primary Input, r - Recirculation
Source/mask      Destination/mask  RPF/DF  Flags #packets      #bytes
rwindeX  Output Vlans/Info
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
*          555151515/35      Df0    BCp   0          0          -
*          555151515/35      -      Bpr   0          0
0x4AE    Vl54,Vl30 [5 oifs]
*          555151515/35      -      Br    0          0
0x40E    Vl54,Vl30 [5 oifs]
*          555151514/35      Df0    BCp   0          0          -
*          555151514/35      -      Bpr   0          0
0x4AE    Vl54,Vl30 [5 oifs]
*          555151514/35      -      Br    0          0
0x40E    Vl54,Vl30 [5 oifs]

Found 5 entries 1 5 are mfd entries
Router#
```

This example shows how to display detailed egress-Bidir information:

```
Router# show mls cef ip multicast bidir detail
```

```
(* , 555151515)
  PI:4 (4) CR:0 (0) Recirc:0 (4)
  DFidx:0 AdjPtr:49,35787,65555,98353 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE6
  rwlans:0 rwindeX:0x0 rdt:0 E:0 CAP4:0
  fmt:recir l3rwld:4 DM:0 mtu:4555 rwtype:RECIR
  packets:000000000000 bytes:000000000000000000

  PI:4 (4) CR:0 (0) Recirc:4 (4)
  AdjPtr:50,35788,65556,98354 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE8
  rwlans:0 rwindeX:0x4AE adjmac:00061d6061e540 rdt:4 E:4 CAP4:0
  fmt:mcast l3rwld:4 DM:0 mtu:4555 rwtype:L3 met5:0x0 met3:0x55
  packets:000000000000 bytes:000000000000000000
  Starting Offset: 0x0055
    V C: 54 I:0x004B3 P->54
    V E C: 30 I:0x004B6

  PI:0 (4) CR:0 (0) Recirc:4 (4)
  AdjPtr:54,35789,65557,98355 FibRpfNf:0 FibRpfDf:0 FibAddr:0xEA
  rwlans:0 rwindeX:0x40E adjmac:00061d6061e540 rdt:4 E:0 CAP4:0
  fmt:mcast l3rwld:4 DM:0 mtu:4555 rwtype:L3 met5:0x0 met3:0x55
  packets:000000000000 bytes:000000000000000000
  Starting Offset: 0x0055
    V C: 54 I:0x004B3 P->54
    V E C: 30 I:0x004B6

(* , 555151514)
  PI:4 (4) CR:0 (0) Recirc:0 (4)
  DFidx:0 AdjPtr:46,35784,65555,98350 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE0
  rwlans:0 rwindeX:0x0 rdt:0 E:0 CAP4:0
  fmt:recir l3rwld:4 DM:0 mtu:4555 rwtype:RECIR
  packets:000000000000 bytes:000000000000000000

  PI:4 (4) CR:0 (0) Recirc:4 (4)
  AdjPtr:47,35785,65553,98354 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE5
  rwlans:0 rwindeX:0x4AE adjmac:00061d6061e540 rdt:4 E:4 CAP4:0
```

## ■ show mls cef ip multicast

```

fmt:mcast l3rwvld:4 DM:0 mtu:4555 rwtpe:L3 met5:0x0 met3:0x4E
packets:000000000000 bytes:0000000000000000
Starting Offset: 0x004E
  V C:  54 I:0x004AF P->50
  V E C:  30 I:0x004B5

PI:0 (4) CR:0 (0) Recirc:4 (4)
AdjPtr:48,35786,65554,98355 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE4
rwlans:0 rwindex:0x40E adjmac:00061d6061e540 rdt:4 E:0 CAP4:0
fmt:mcast l3rwvld:4 DM:0 mtu:4555 rwtpe:L3 met5:0x0 met3:0x4E
packets:000000000000 bytes:0000000000000000
Starting Offset: 0x004E
  V C:  54 I:0x004AF P->50
  V E C:  30 I:0x004B5

```

```

Found 5 entries 5 are mfd entries
Router#

```

This example shows how to display TCAM information:

```

Router# show mls cef ip multicast tcam

```

Index	Group	Source	RPF/DF	Interface
64	5541014139	0101010	NULL	
66	5541014140	0101010	NULL	
96	554101010	0101010	NULL	

```

Router#

```

# show mls cef ipv6

To display the hardware IPv6-switching table entries, use the **show mls cef ipv6** command.

```
show mls cef ipv6 [vrf-number] [ip-address/mask] [accounting per-prefix] [module number]
```

```
show mls cef ipv6 exact-route src-addr [L4-src-port] dst-addr [L4-dst-port]
```

```
show mls cef ipv6 multicast team [v6mcast-address] [detail] [internal]
```

## Syntax Description

<i>vrf-number</i>	(Optional) VRF number; valid values are from 0 to 4095.
<i>ip-address/mask</i>	(Optional) Entry IPv6 address and prefix mask; see the “Usage Guidelines” section for formatting information.
<b>accounting per-prefix</b>	(Optional) Displays per-prefix accounting statistics.
<b>module number</b>	(Optional) Displays the entries for a specific module.
<b>exact-route</b> <i>src-addr</i>	Specifies the source IP address to display the hardware load sharing results.
<i>L4-src-port</i>	(Optional) Layer 4-source port number; valid values are from 0 to 65535.
<i>dst-addr</i>	Destination IP address.
<i>L4-dst-port</i>	(Optional) Layer 4-destination port number; valid values are from 0 to 65535.
<b>multicast team</b>	Displays IPv6-multicast entries.
<i>v6mcast-address</i>	(Optional) IPv6-multicast address.
<b>detail</b>	(Optional) Displays detailed hardware information.
<b>internal</b>	(Optional) Displays internal hardware information.

## Defaults

This command has no default settings.

## Command Modes

EXEC

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

You can enter this command on the supervisor engine and MLS-hardware Layer 3-switching module consoles only. Enter the **remote login** command to session into the supervisor engine to enter the commands.

When entering the *ip-address/mask* argument, use this format, X:X:X:X:X/mask, where valid values for *mask* are from 0 to 128.

Up to 64 IPv6 prefixes are supported.

You must enter the *L4-src-port* and *L4-dst-port* arguments when the load-sharing mode is set to full, for example, when Layer 4 ports are included in the load-sharing hashing algorithm.

## Examples

This example shows how to display the hardware IPv6-switching table entries:

```
Router# show mls cef ipv6
Codes:M-MPLS encap, + - Push label
Index Prefix Adjacency
554384 BEEF:6::6/458 punt
554386 5500::6/458 punt
554388 5959::6/458 punt
554390 6363::30/458 Fa4/48 , 00001000410005
554395 3FFE:4B00:4:4:0:5EFE:4B00:4/458 punt
554394 5005:5959:6:5::6/458 punt
554396 5005:5959:6:4::6/458 punt
554398 6363::6/458 punt
554446 BEEF:6::/64 drop
554448 5500::/64 punt
554450 5959::/64 punt
554455 5005:5959:6:5::/64 punt
554454 5005:5959:6:4::/64 punt
554456 6363::/64 punt
554458 3FFE:4B00:4:4::/64 Tu4 , V6 auto-tunnel
554448 FEEO::/44 punt
554480 FE80::/40 punt
554545 FF00::/8 punt
554544 ::/0 drop
Router#
```

This example shows how to display the IPv6 entries for a specific IPv6 address and mask:

```
Router# show mls cef ipv6 2001:4747::/64

Codes:R - Recirculation, I-IP encap
M-MPLS encap, + - Push label
Index Prefix Out i/f Out Label
460 5004:4747::/64 punt
Router#
```

This example shows how to display all the IPv6-FIB entries that have per-prefix statistics available:

```
Router# show mls cef ipv6 accounting per-prefix
(I) BEEF:5::/64: 0 packets, 0 bytes

A - Active, I - Inactive
Router#
```

This example shows how to display detailed hardware information:

```
Router# show mls cef ipv6 detail

Codes: M - mask entry, V - value entry, A - adjacency index, P - FIB Priority
D - FIB Don't short-cut, m - mod-num
Format: IPv6_DA - (C ; xtag vpn uvo prefix)
M(458 ): F ; 4 FF 4 FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
V(458 ): C ; 4 0 4 5004:4747::4553 (A:45 ,P:4,D:0,m:0 )
M(460 ): F ; 4 FF 4 FFFF:FFFF:FFFF:FFFF:
V(460 ): C ; 4 0 4 5004:4747:: (A:44 ,P:4,D:0,m:0 )
```

```

M(554 ) : F ; 4 FF 4 FFE0::
V(554 ) : C ; 4 0 4 FEE0:: (A:44 ,P:4,D:0,m:0 )
M(556 ) : F ; 4 FF 4 FFC0::
V(556 ) : C ; 4 0 4 FE80:: (A:45 ,P:4,D:0,m:0 )
M(355 ) : F ; 4 FF 4 FF00::
V(355 ) : C ; 4 0 4 FF00:: (A:45 ,P:4,D:0,m:0 )
M(480 ) : F ; 4 FF 4 ::
V(480 ) : C ; 4 0 4 :: (A:44 ,P:4,D:0,m:0
Router#

```

**Related Commands**

Command	Description
<a href="#">mls ipv6 acl compress address unicast</a>	Turns on the compression of IPv6 addresses.

# show mls cef logging

To display the contents of the TCAM-inconsistency buffer, use the **show mls cef logging** command.

**show mls cef logging** [*module num*]

<b>Syntax Description</b>	<b>module num</b> (Optional) Displays the entries for a specific module.
---------------------------	--

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	The TCAM-inconsistency buffer records any inconsistency that is found in the TCAM. MLS-hardware Layer 3 switching applies to IP traffic only.
-------------------------	---

<b>Examples</b>	This example shows how to display the contents of the TCAM inconsistency buffer:
-----------------	--

```
Router# show mls cef logging
PFIB_ERR:TCAM_SHADOW_CONSISTENC\_ERR:value : Index: 400
Expected: 0 -0 -0
Hardware: 5 -4050304 -0
PFIB_ERR:TCAM_SHADOW_CONSISTENC\_ERR:Mask : Index: 3
Expected: 4 -0 -0
Hardware: 6 -FFF00000-0
Router#
```

# show mls cef lookup

To display the IP entries in the MLS-hardware Layer 3-switching table for the specified destination IP address, use the **show mls cef lookup** command.

```
show mls cef [ip] lookup address [detail] [module number]
```

Syntax Description	ip	(Optional) Displays IP entries in the MLS-hardware Layer 3-switching table; see the “Usage Guidelines” section for additional information.
	address	IP address in the format A.B.C.D.
	detail	(Optional) Displays hardware-entry details.
	module number	(Optional) Displays the entries for a specific module.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The lookup is performed as a “longest-prefix match” and displays the TCAM-entry index that applies to the specified destination IP address.

The information output is in this format: Index, Prefix, Mask, and Adjacency.

The output of the **show mls cef lookup ip** and the **show mls cef lookup** commands is identical.

**Examples** This example shows how to display the longest prefix match that applies to a specific IPv4-unicast address:

```
Router# show mls cef lookup 224.0.0.0

Codes: decap - Decapsulation, + - Push Label
Index Prefix Adjacency
3500 554101010/54 punt
Router#
```

# show mls cef maximum-routes

To view the current maximum-route system configuration, use the **show mls cef maximum-routes** command.

## show mls cef maximum-routes

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

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** When you enter the **mls cef maximum-routes** command to change the configuration, the following additional fields appear in the output of the **show mls cef maximum-routes** command:

- User configured—Shows configuration changes that you have made.
- Upon reboot—Shows the configuration after a system reboot.

These fields appear if you have not saved the change (using the **copy system:running-config nvram:startup-config** command) after entering the **mls cef maximum-routes** command. See the “Examples” section for additional information.

**Examples** This example shows the display after you have entered the **mls cef maximum-routes** command, saved the change (**copy system:running-config nvram:startup-config** command), and rebooted the system:

```
Router# show mls cef maximum-routes
FIB TCAM maximum routes :
=====
Current :-
-----
IPv4 - 4k (default)
MPLS - 539k
IPv6 + IP Multicast - 8k (default)
Router#
```

This example shows the display if you entered the **mls cef maximum-routes** command and did not save the change:

```
Router# show mls cef maximum-routes
FIB TCAM maximum routes :
=====
Current :-
-----
IPv4 - 4k (default)
```

```

MPLS - 539k
IPv6 + IP Multicast - 8k (default)
User configured :-
-----
IPv4 + MPLS - 495k (default)
IPv6 + IP multicast - 35k (default)
Upon reboot :-
-----
IPv4 - 4k (default)
MPLS - 539k
IPv6 + IP multicast - 8k (default)
Router#

```

This example shows the output if you have made a configuration change and saved the change (**copy system:running-config nvram: startup-config** command):

```

Router# show mls cef maximum-routes
FIB TCAM maximum routes :
=====
Current :-
-----
IPv4 - 4k (default)
MPLS - 539k
IPv6 + IP Multicast - 8k (default)
User configured :-
-----
IPv4 + MPLS - 495k (default)
IPv6 + IP multicast - 35k (default)
Router#

```

#### Related Commands

Command	Description
<b>copy</b> <b>system:running-config</b> <b>nvram: startup-config</b>	Saves the configuration to NVRAM.
<b>mls cef</b> <b>maximum-routes</b>	Limits the maximum number of the routes that can be programmed in the hardware allowed per protocol.

# show mls cef mpls

To display the MPLS entries in the MLS-hardware Layer 3-switching table, use the **show mls cef mpls** command.

```
show mls cef mpls [detail] [internal] [labels value] [module number] [vpn instance]
                 [vrf instance]
```

Syntax Description	Parameter	Description
	<b>detail</b>	(Optional) Displays hardware-entry details.
	<b>internal</b>	(Optional) Displays internal CEF entries.
	<b>labels value</b>	(Optional) Displays the entries for a specific label; valid values are from 0 to 1048575.
	<b>module number</b>	(Optional) Displays the entries for a specific module.
	<b>vpn instance</b>	(Optional) Displays the VPN ID MPLS table entries for a specific VPN instance; valid values are from 0 to 4095.
	<b>vrf instance-name</b>	(Optional) Displays the MPLS CEF table entries for a specific VRF.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This examples shows how to display MPLS entries:

```
Router# show mls cef mpls

Codes: + - Push label, - - Pop Label          * - Swap Label
Index  Local  Label          Out i/f
      Label    Op
Router#
```

# show mls cef rpf

To display the information about the RPF hardware in the MLS-hardware Layer 3-switching table, use the **show mls cef rpf** command.

```
show mls cef [ip] rpf [ip-address] [module num]
```

Syntax Description	ip	(Optional) Displays IP entries in the MLS-hardware Layer 3-switching table; see the “Usage Guidelines” section for additional information.
	<i>ip-address</i>	(Optional) IP address.
	<b>module num</b>	(Optional) Displays the entries for a specific module.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** If you enter the **show mls cef ip rpf** command without arguments, the RPF global mode status is displayed.

The output of the **show mls cef ip rpf** and the **show mls cef rpf** commands is identical.

**Examples** This example shows how to display the status of the RPF global mode:

```
Router# show mls cef rpf

RPF global mode:      not enabled
Router#
```

This example shows how to display the RPF information for a specific IP address:

```
Router# show mls cef rpf 10.100.0.0
RPF information for prefix 4014001010/54
uRPF check performed in the hardware for interfaces :
GigabitEthernet4/4
Router#
```

Related Commands	Command	Description
	<a href="#">mls ip cef rpf multipath</a>	Configures the RPF modes.

# show mls cef statistics

To display the number of switched packets and bytes, use the **show mls cef statistics** command.

**show mls cef statistics** [*module number*]

<b>Syntax Description</b>	<b>module number</b> (Optional) Displays the information for a specific module.
---------------------------	---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Examples</b>	This example shows how to display the MLS-hardware Layer 3-switching statistics:
-----------------	--

```
Router# show mls cef statistics

Total CEF switched packets: 0000000000000000
Total CEF switched bytes:   0000000000000000
Router#
```

# show mls cef summary

To display the number of routes in the MLS-hardware Layer 3-switching table for all the protocols, use the **show mls cef summary** command.

**show mls cef summary** [*module number*]

<b>Syntax Description</b>	<b>module number</b> (Optional) Displays the information for a specific module.
---------------------------	---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	The number of prefixes in the MLS-hardware Layer 3-switching table indicates the individual numbers for IPv4 and IPv6 unicast, IPv4 multicast, MPLS, and EoM routes.
-------------------------	--

<b>Examples</b>	This example shows how to display a summary of MLS-hardware Layer 3-switching information:
-----------------	--

```
Router# show mls cef summary
Total routes:                80385
  IPv4 unicast routes:        45
  IPv4 Multicast routes:      5
  MPLS routes:                0
  IPv6 unicast routes:        5
  EoM routes:                 0
Router#
```

[Table 2-82](#) describes the fields in the **show mls cef summary** command output.

**Table 2-82** *show mls cef summary* Command Output Fields

Field	Description
Total MLS-hardware Layer 3-switching switched packets	Number of MLS-hardware Layer 3-switching packets forwarded by the MLS-hardware Layer 3-switching engine.
Total MLS-hardware Layer 3-switching switched bytes	Number of bytes forwarded by the MLS-hardware Layer 3-switching engine.
Total routes	Number of route entries.
IP unicast routes	Number of IP-unicast route entries.

*Table 2-82 show mls cef summary Command Output Fields (continued)*

Field	Description
IPX routes	Number of IPX route entries.
IP multicast routes	Number of IP-multicast route entries.

**Related Commands**

Command	Description
<a href="#">show mls cef</a>	Displays the MLS-hardware Layer 3-switching table entries.

## show mls cef vrf

To display information about the VPN routing and forwarding instance CEF table for a specific VRF name, use the **show mls cef vrf** command.

```
show mls cef vrf instance-name [prefix] [detail] [lookup ip-address] [module num]
[rpf [ip-address]]
```

Syntax Description	
<i>instance-name</i>	VPN routing/forwarding instance name; valid values are from 0 to 4095.
<i>prefix</i>	(Optional) Prefix of the entry to display.
<b>detail</b>	(Optional) Displays the hardware-entry details.
<b>lookup</b> <i>ip-address</i>	(Optional) Displays the longest prefix-match lookup entry for the specified address.
<b>module</b> <i>num</i>	(Optional) Displays the entries for a specific module.
<b>rpf</b> <i>ip-address</i>	(Optional) Displays the uRPF check information for the (optional) specified IP address.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **show mls cef ip** command displays the CEF entries in the default VRF. To display specific (nondefault) VRF entries, use the **show mls cef [ip] vrf vrf-name** command.

**Examples** This example shows how to display information about the VPN routing and forwarding instance CEF table for a specific VRF name:

```
Router# show mls cef vrf vpn-1

Codes: decap - Decapsulation, + - Push Label
Index Prefix Adjacency
64 0101010/35 receive
65 555155515551555/35 receive
580 715015714/35 receive
584 715015710/35 receive
585 71501571555/35 receive
598 5141414/35 receive
```

## ■ show mls cef vrf

```
599 5141410/35 receive
300 514141555/35 receive
656 51419914/35 receive
Router#
```

## Related Commands

Command	Description
<a href="#">show mls cef ip</a>	Displays the IP entries in the MLS-hardware Layer 3-switching table.

# show mls df-table

To display information about the DF table, use the **show mls df-table** command.

**show mls df-table** *start-vlan end-vlan*

Syntax Description	
<i>start-vlan</i>	Start of a range of VLAN IDs; valid values are from 1 to 4094.
<i>end-vlan</i>	End of a range of VLAN IDs; valid values are from 1 to 4094.

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

**Command Modes** Switch processor—EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** In the output display, the following applies:

- 1 indicates that DF is enabled.
- 0 indicates that DF is disabled.

**Examples** This example shows how to display the DF-table contents for a range of VLANs:

```
Switch-sp# show mls df-table 201 212
T\CHO FIB DF Table

vlan    df_index
      3 5 4 0
-----+-----
504    4 4 4 4
505    4 4 4 4
503    4 4 4 4
504    4 4 4 4
505    4 4 4 4
506    4 4 4 4
507    4 4 4 4
508    4 4 4 4
509    4 4 4 4
540    4 4 4 4
544    4 4 4 4
545    4 4 4 4
Switch-sp#
```

# show mls ip

To display the MLS IP information, use the **show mls ip** command.

```
show mls ip [any | destination {hostname | ip-address} | detail | flow {tcp | udp} | {vlan vlan-id}
| {macd destination-mac-address} | {macs source-mac-address} | {module number} |
source {hostname | ip-address} | count | static]
```

```
show mls {ipv6 | mpls}
```

Syntax Description	
<b>any</b>	(Optional) Displays any MLS IP information.
<b>destination</b> <i>hostname</i>	(Optional) Displays the entries for a specific destination hostname.
<b>destination</b> <i>ip-address</i>	(Optional) Displays the entries for a specific destination IP address.
<b>detail</b>	(Optional) Specifies a detailed output.
<b>flow</b>	(Optional) Specifies the flow type.
<b>tcp   udp</b>	Selects the flow type.
<b>vlan</b> <i>vlan-id</i>	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.
<b>macd</b> <i>destination-mac-address</i>	(Optional) Specifies the destination MAC address.
<b>macs</b> <i>source-mac-address</i>	(Optional) Specifies the source MAC address.
<b>module</b> <i>number</i>	(Optional) Displays the entries that are downloaded on the specified module; see the “Usage Guidelines” section for valid values.
<b>source</b> <i>hostname</i>	(Optional) Displays the entries for a specific source address.
<b>source</b> <i>ip-address</i>	(Optional) Displays the entries for a specific source IP address.
<b>count</b>	(Optional) Displays the total number of MLS entries.
<b>static</b>	(Optional) Displays the total number of static entries.
<b>ipv6</b>	Displays the total number of IPv6 entries.
<b>mpls</b>	Displays the total number of MPLS entries.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.



## ■ show mls ip

```

-----+-----+-----+-----+-----+-----+-----+-----+
4571010149      4571010146      udp :68      :67      4009: 0x0
75      3345      4470 50:43:54  L3 - Dynamic
0  4  0  0  4  0  0  4  4  0  0  0  0
0      0  0  0  0  0  0  0  0  0  0
      0x0      0      0      0      NO 64      NO      NO
Router#

```

## Related Commands

Command	Description
<a href="#">mls ip</a>	Enables MLS IP for the internal router on the interface.
<a href="#">show mls netflow ip</a>	Displays information about the hardware NetFlow IP.

# show mls ip cef rpf-table

To display the configuration of the RPF CEF table, use the **show mls ip cef rpf-table** command.

## show mls ip cef rpf-table

<b>Syntax Description</b>	This command has no keywords or arguments.
---------------------------	--

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Examples</b>	This example shows how to display the RPF CEF-table entries:
-----------------	--

```
Router# show mls ip cef rpf-table
-----
47514014010/54      [0] Fa5/4, Fa5/5, Fa5/3, Fa5/4
47514015010/54
47514013010/54
401401010/46      [4] Gi4/4, Gi4/5
401501010/46
Router#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">mls ip cef rpf interface-group</a>	Defines an interface group in the RPF-VLAN table.

# show mls ip multicast

To display the MLS IP information, use the **show mls ip multicast** command.

```
show mls ip multicast [{capability [module num]} | connected | group] [{hostname | ip-address}
  [ip-mask]}] | {interface {interface interface-number}} | {module number} | mdt |
  {source {hostname | ip-address}} | statistics | summary]
```

```
show mls ip multicast consistency-check [mroute-mlsm | {rp-sp [log [clear] | statistics]}]
```

## Syntax Description

<b>capability</b>	Displays information about the multicast-replication capabilities.
<b>module num</b>	(Optional) Specifies the module number.
<b>connected</b>	(Optional) Displays the installed interface or mask entries.
<b>group</b>	(Optional) Displays the entries for a specific multicast-group address.
<i>hostname</i>	Group IP hostname.
<i>ip-address</i>	Group IP address.
<i>ip-mask</i>	(Optional) IP mask for group IP address.
<b>interface</b>	(Optional) Specifies an interface.
<i>interface</i>	Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , <b>atm</b> , and <b>ge-wan</b> .
<i>interface-number</i>	Module and port number; see the “Usage Guidelines” section for valid values.
<b>module number</b>	(Optional) Displays the entries that are downloaded on the specified module; see the “Usage Guidelines” section for valid values.
<b>mdt</b>	(Optional) Displays hardware-accelerated MDT information.
<b>source hostname</b>	(Optional) Displays the entries for a specific source address.
<b>source ip-address</b>	(Optional) Displays the entries for a specific source IP address.
<b>statistics</b>	(Optional) Displays the statistics from multicast entries.
<b>summary</b>	(Optional) Displays a summary of statistics from multicast entries.
<b>consistency-check</b>	Displays consistency-checker information.
<b>mroute-mlsm</b>	(Optional) Displays mroute/MLSM consistency-checker information.
<b>rp-sp</b>	(Optional) Displays route processor/switch processor consistency-checker information.
<b>log</b>	(Optional) Displays a log of mismatches that have been detected and corrected.
<b>clear</b>	(Optional) Clears the mismatches log.
<b>statistics</b>	(Optional) Displays the statistics of prefixes checked.

## Defaults

This command has no default settings.

## Command Modes

EXEC

**Command History**

Release	Modification
12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48. These valid values also apply when entering the **module number** keyword and argument.

When you view the output, note that a colon (:) is used to separate the fields.

**Examples**

This example shows how to display general MLS IP-multicast information:

```
Router# show mls ip multicast
Multicast hardware switched flows:
(*, 554141414) Incoming interface: Vlan0, Packets switched: 0
Hardware switched outgoing interfaces: Vlan505
RPF-MFD installed
Total hardware switched flows : 4
Router#
```

This example shows how to display a summary of MLS information:

```
Router# show mls ip multicast summary
4 MMLS entries using 468 bytes of memory
Number of partial hardware-switched flows: 0
Number of complete hardware-switched flows: 4
Directly connected subnet entry install is enabled
Aggregation of routed oif is enabled
Hardware shortcuts for mvpn mroutes supported
Egress Mode of replication is enabled
Maximum route support is enabled
Router#
```

This example shows how to display MLS information on a specific interface:

```
Router# show mls ip multicast interface fastethernet 5/9
DstIP          SrcIP          Dst i/f:DstMAC  Pkts          Bytes
-----
SrcDstPorts    SrcDstEncap Age    LastSeen
-----
475150155137   0101010        400: 00d0158701a4ff 4              459
Fa5/9,----- ARPA,ARPA    407    06:40:05
475150155136   0101010        400 : 00501734510cff 50             6403
Fa5/9,----- ARPA,ARPA    407    06:40:04
Number of Entries Found = 5
Router#
```

This example shows how to display information about the multicast-replication capabilities:

```
Router# show mls ip multicast capability
Current mode of replication is Ingress
auto replication mode detection is ON

Slot          Multicast replication capability
5              Egress
5              Egress
6              Egress
```

## ■ show mls ip multicast

```

      8                Ingress
      9                Ingress
Router#

```

This example shows how to display information about the mroute consistency-checker log:

```

Router# show mls ip multicast consistency-check mroute-mlsm
MMLS Consistency checker of mroute-scan type is enabled
Inter scan period = 5 sec
Number of entry scanned = 50
Settle time = 60 sec
Storage for 4000 events (40000 bytes)
Mroute entry missed for a Shortcut : 0
Mroute entry was uneligible for a Shortcut : 0
Mroute entry rpf i/f mismatched with Shortcut : 0
Mroute oif in hw and Shortcut oif in sw : 0
Mroute oif in sw and Shortcut oif in sw : 0
Mroute oif in sw and Shortcut oif in hw : 0
Mroute #oif mismatched with Shortcut #oif : 0
1
1
1
<Output is truncated>

```

This example shows how to display a log of mismatches that have been detected and corrected:

```

Router# show mls ip multicast consistency-check rp-sp log
MLSM RP<->SP Consistency Checker Mismatch log for Table 0:
size 545 current-index 0

0 total used entries in log
Router#

```

## Related Commands

Command	Description
<b>mls ip multicast (interface configuration mode)</b>	Enables MLS IP shortcuts on the interface.

# show mls ip multicast bidir

To display the Bidir hardware-switched entries, use the **show mls ip multicast bidir** command.

```
show mls ip multicast bidir [{group {hostname | ip-address} [ip-mask]}] | {interface {interface
interface-number}} | {source {hostname | ip-address}}]
```

Syntax Description	group	(Optional) Displays the entries for a specific multicast-group address.
	<i>hostname</i>	Group IP hostname.
	<i>ip-address</i>	Group IP address.
	<i>ip-mask</i>	(Optional) IP mask for group IP address.
	<b>interface</b>	(Optional) Specifies an interface.
	<i>interface</i>	Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , and <b>tengigabitethernet</b> .
	<i>interface-number</i>	Module and port number; see the “Usage Guidelines” section for valid values.
	<b>source hostname</b>	(Optional) Displays the entries for a specific source address.
	<b>source ip-address</b>	(Optional) Displays the entries for a specific source IP address.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the Bidir hardware-switched entries:

```
Router# show mls ip multicast bidir
Multicast hardware switched flows:
(*, 556141410) Incoming interface: Vlan54, Packets switched: 0
Hardware switched outgoing interfaces: Vlan54 Vlan30
RPF-MFD installed
(*, 557141410) Incoming interface: Gi5/4, Packets switched: 0
Hardware switched outgoing interfaces: Gi5/4 Vlan30
RPF-MFD installed
Router#
```

Related Commands	Command	Description
	<a href="#">mls ip multicast bidir gm-scan-interval</a>	Sets the RPF scan interval for the Bidir rendezvous point.

## show mls ip multicast rp-mapping

To display the mappings for the PIM-Bidir group to active rendezvous points, use the **show mls ip multicast rp-mapping** command.

```
show mls ip multicast rp-mapping [rp-address] [df-cache | gm-cache]
```

Syntax Description	
<i>rp-address</i>	(Optional) Rendezvous-point address.
<b>df-cache</b>	(Optional) Displays information on the DF list in the rendezvous-point mapping cache in the hardware.
<b>gm-cache</b>	(Optional) Displays information on the group/mask ranges in the rendezvous-point mapping cache in the hardware.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the mappings for the PIM group-to-active rendezvous points:

```
Router# show mls ip multicast rp-mapping
RP Address State DF-count GM-count
5151515 H 4 4
9191919 H 4 5
Router#
```

This example shows how to display information that is based on the DF list in the mapping cache of the route processor:

```
Router# show mls ip multicast rp-mapping df-cache
RP Address State DF State
9191919 H V130 H
Router#
```

This example shows how to display information that is based on the mapping cache of the route processor:

```
Router# show mls ip multicast rp-mapping gm-cache
State: H - Hardware Switched, I - Install Pending, D - Delete Pending,
J - Jombie
RP Address State Group Mask State Packet/Byte-count
601010160 H 5301341010 55515551010 H 400/6400
Router#
```

# show mls ip multicast sso

To display information about multicast high-availability SSO, use the **show mls ip multicast sso** command.

**show mls ip multicast sso [statistics]**

Syntax Description	<b>statistics</b> (Optional) Displays multicast high-availability SSO statistical information.
--------------------	--

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display multicast high-availability SSO information:

```
Router> show mls ip multicast sso
Multicast SSO is enabled
Multicast HA Parameters
-----+-----
protocol convergence timeout          450 secs
flow leak percent                     40
flow leak interval                   50 secs
heartquake#
```

This example shows how to display statistical information about multicast high-availability SSO:

```
Router# show mls ip multicast sso statistics

Multicast HA Statistics: ACTIVE
-----+-----
CHKPT msgs sent                      5
CHKPT msgs send failed                0
CHKPT msgs send aborted              0
CHKPT met add msg sent                5
CHKPT met del msg sent                4
CHKPT icroif msg sent                4
MET HA met add enqueued               5
MET HA met del enqueued               4
ICROIF HA add enqueued                4
ICROIF HA del enqueued                0
CHKPT buffer failure                  0

MET HA Reconstruction Statistics
-----+-----
Number of met blks reconstructed      0
Number of normal sets reconstructed   0
Number of fixed sets reconstructed    0
Number of sets deleted                 0
```

## ■ show mls ip multicast sso

```

Number of blks not found          0
normal sets reconstruction failed  0
fixed set reconstruction failed    0

Multicast HA Statistics: STANDB\
-----+-----+
CHKPT msgs rcvd                   5
CHKPT met add msg rcvd             5
CHKPT met del msg rcvd             4
CHKPT icroif msg rcvd             4
CHKPT msg unknown                  0
CHKPT buffer failure               0
Router#

```

## Related Commands

Command	Description
<a href="#">mls ip multicast sso</a>	Configures the SSO parameters.

# show mls ip non-static

To display information for the software-installed nonstatic entries, use the **show mls ip non-static** command.

**show mls ip non-static** [**count** [**module number**] | **detail** [**module number**] | **module number**]

Syntax Description	
<b>count</b>	(Optional) Displays the total number of nonstatic entries.
<b>module number</b>	(Optional) Designates the module number.
<b>detail</b>	(Optional) Specifies a detailed per-flow output.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the software-installed nonstatic entries:

```
Router> show mls ip non-static
Displaying Netflow entries in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts          Bytes          Age  LastSeen  Attributes
-----
Router>
```

This example shows how to display detailed information for the software-installed nonstatic entries:

```
Router> show mls ip non-static detail
Displaying Netflow entries in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts          Bytes          Age  LastSeen  Attributes
-----
QoS    Police Count Threshold  Leak    Drop Bucket  Use-Tbl Use-Enable
-----+-----+-----+-----+-----+-----+-----+
Router>
```

This example shows how to display the total number of software-installed nonstatic entries:

```
Router> show mls ip non-static count
Displaying Netflow entries in Supervisor Earl

Number of shortcuts = 0
Router>
```

# show mls ip routes

To display the NetFlow routing entries, use the **show mls ip routes** command.

```
show mls ip routes [non-static | static] [count [module number] | detail [module number] |
module number]
```

Syntax Description	
<b>non-static</b>	(Optional) Displays the software-installed nonstatic entries.
<b>static</b>	(Optional) Displays the software-installed static entries.
<b>count</b>	(Optional) Displays the total number of NetFlow routing entries.
<b>module number</b>	(Optional) Displays the entries that are downloaded on the specified module; see the “Usage Guidelines” section for valid values.
<b>detail</b>	(Optional) Specifies a detailed per-flow output.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the software-installed nonstatic routing entries:

```
Router> show mls ip routes non-static
Displaying Netflow entries in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts          Bytes          Age  LastSeen  Attributes
-----
Router>
```

This example shows how to display detailed information for the software-installed nonstatic routing entries:

```
Router> show mls ip routes non-static detail
Displaying Netflow entries in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts          Bytes          Age  LastSeen  Attributes
-----
QoS          Police Count Threshold  Leak  Drop Bucket  Use-Tbl Use-Enable
-----+-----+-----+-----+-----+-----+-----+-----+
Router>
```

This example shows how to display the total number of software-installed routing entries:

```
Router> show mls ip routes count
Displaying Netflow entries in Supervisor Earl

Number of shortcuts = 0
Router>
```

---

**Related Commands**

Command	Description
<a href="#">show mls netflow ip sw-installed</a>	Displays information for the software-installed IP entries.

---

# show mls ip static

To display the information for the software-installed static IP entries, use the **show mls ip static** command.

**show mls ip static** [**count** [**module number**] | **detail** [**module number**] | **module number**]

Syntax Description	count	(Optional) Displays the total number of static entries.
	<b>module number</b>	(Optional) Designates the module number.
	<b>detail</b>	(Optional) Specifies a detailed per-flow output.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the software-installed static entries:

```
Router> show mls ip static
Displaying Netflow entries in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts          Bytes          Age  LastSeen  Attributes
-----
Router>
```

This example shows how to display detailed information for the software-installed static entries:

```
Router> show mls ip static detail
Displaying Netflow entries in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts          Bytes          Age  LastSeen  Attributes
-----
          QoS      Police Count Threshold  Leak      Drop Bucket  Use-Tbl Use-Enable
-----+-----+-----+-----+-----+-----+-----+-----+
Router>
```

This example shows how to display the total number of software-installed static entries:

```
Router> show mls ip static count
Displaying Netflow entries in Supervisor Earl

Number of shortcuts = 0
Router>
```

# show mls ip statistics

To display the statistical information for the NetFlow IP entries, use the **show mls ip statistics** command.

**show mls ip statistics** [**count** [*module number*] | **detail** [*module number*] | **module** *number*]

Syntax Description	
<b>count</b>	(Optional) Displays the total number of NetFlow entries.
<b>module</b> <i>number</i>	(Optional) Displays the entries that are downloaded on the specified module.
<b>detail</b>	(Optional) Specifies a detailed per-flow output.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display statistical information for the NetFlow IP entries:

```
Router> show mls ip statistics
Displaying Netflow entries in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts          Bytes          Age  LastSeen  Attributes
-----
Router>
```

This example shows how to display detailed statistical information for the NetFlow IP entries:

```
Router> show mls ip statistics detail
Displaying Netflow entries in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts          Bytes          Age  LastSeen  Attributes
-----
          QoS      Police Count Threshold  Leak      Drop Bucket  Use-Tbl Use-Enable
-----+-----+-----+-----+-----+-----+-----+
Router>
```

# show mls nde

To display information about the NDE hardware-switched flow, use the **show mls nde** command.

**show mls nde**

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

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The output for Catalyst 6500 series switches includes the current NDE mode.

**Examples** This example shows how to display information about the NDE hardware-switched flow on a Catalyst 6500 series switch:

```
Router# show mls nde
Netflow Data Export enabled (Interface Mode)
Exporting flows to 475150155174 (9994)
Exporting flows from 40161601450 (59050)
Version: 7
Include Filter not configured
Exclude Filter not configured
Total Netflow Data Export Packets are:
  0 packets, 0 no packets, 0 records
Router#
```

Related Commands	Command	Description
	<a href="#">mls nde sender</a>	Enables MLS NDE export.
	<a href="#">show ip flow-export</a>	Displays the information about the hardware-switched and software-switched flows for the data export, including the main cache and all other enabled caches.
	<a href="#">show mls netflow</a>	Displays configuration information about the NetFlow hardware.

# show mls netflow

To display configuration information about the NetFlow hardware, use the **show mls netflow** command.

```
show mls netflow {aging | aggregation flowmask | creation | flowmask | {table-contention
{detailed | summary}} | usage}
```

```
show mls netflow [ip | ipv6 | mpls] [any | count | destination {hostname | ip-address} | detail |
dynamic | flow {tcp | udp} | module number / nowrap | source {hostname | ip-address} |
sw-installed [non-static | static]]
```

Syntax	Description
<b>aging</b>	Displays the NetFlow-aging information.
<b>aggregation flowmask</b>	Displays the flow mask that is set for the current NetFlow aggregations.
<b>creation</b>	Displays the configured protocol-creation filters.
<b>flowmask</b>	Displays the current NetFlow IP and IPX flow mask.
<b>table-contention</b>	Displays the NetFlow table-contention level information.
<b>detailed</b>	Displays detailed NetFlow table-contention level information.
<b>summary</b>	Displays a summary of NetFlow table-contention levels.
<b>usage</b>	Displays the NetFlow table-usage notification status.
<b>ip</b>	(Optional) Displays information about the NetFlow IP table; see the <a href="#">show mls netflow ip</a> command.
<b>ipv6</b>	(Optional) Displays information about the NetFlow IPv6 table; see the <a href="#">show mls netflow ipv6</a> command.
<b>mpls</b>	(Optional) Displays information about the NetFlow MPLS table.
<b>any</b>	(Optional) Displays detailed NetFlow table-entry information with no test wrap.
<b>count</b>	(Optional) Displays the total number of MLS NetFlow IP entries.
<b>destination hostname</b>	(Optional) Displays the entries for a specific destination hostname.
<b>destination ip-address</b>	(Optional) Displays the entries for a specific destination IP address.
<b>detail</b>	(Optional) Specifies a detailed output.
<b>dynamic</b>	(Optional) Displays the hardware-created dynamic entries.
<b>flow tcp</b>	(Optional) Displays information about the TCP flows.
<b>flow udp</b>	(Optional) Displays information about the UDP flows.
<b>module number</b>	(Optional) Displays the entries that are downloaded on the specified module; see the “Usage Guidelines” section for valid values.
<b>nowrap</b>	(Optional) Displays information without text wrap.
<b>source hostname</b>	(Optional) Displays the entries for a specific source address.
<b>source ip-address</b>	(Optional) Displays the entries for a specific source IP address.
<b>sw-installed</b>	(Optional) Displays the routing NetFlow entries; see the <a href="#">show mls netflow ip sw-installed</a> command.

<b>non-static</b>	(Optional) Displays information for software-installed static IP entries; see the <a href="#">show mls netflow ip sw-installed</a> command.
<b>static</b>	(Optional) Displays information for the software-installed nonstatic IP entries; see the <a href="#">show mls netflow ip sw-installed</a> command.

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

**Command Modes** EXEC

Release	Modification
12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **interface**, **macd**, and **macs** keywords are not supported.

If you enter the **show mls netflow ip** command with no argument, the output of the **show mls netflow ip routes** and **show mls netflow ip dynamic** commands are displayed.

When you view the output, note that a colon (:) is used to separate the fields.

If you enable the NetFlow table-usage notification and the NetFlow table-usage exceeds a preset percentage threshold, a warning message is displayed. You can use the [mls netflow usage notify](#) command to set the threshold percentage and the time interval to check the NetFlow table usage.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48. These valid values also apply when entering the **module number** keyword and argument.

**Examples** This example shows how to display the NetFlow-aging configuration:

```
Router# show mls netflow aging
           enable timeout  packet threshold
           -----
normal aging true         300         N/A
fast  aging  true         35          400
long  aging  true         900         N/A
Router#
```

This example shows how to display the configured protocol-creation filters:

```
Router# show mls netflow creation
Excluded protocols:
port protocol
-----+-----
40      tcp
8       udp/tcp
Router#
```

This example shows how to display the flow mask that is set for the current NetFlow aggregation:

```
Router# show mls netflow aggregation flowmask
Current flowmask set for netflow aggregation : Dest only
Minimum flowmask required for netflow aggregation schemes
-----+-----+-----
Aggregation Scheme Min1 Flowmask Status
-----+-----+-----
as Intf Src Dest disabled
protocol-port Full Flow disabled
source-prefix Intf Src Dest disabled
destination-prefix Dest only enabled
prefix Intf Src Dest disabled
Router#
```

This example shows how to display detailed information about the NetFlow table-contention level:

```
Router# show mls netflow table-contention detailed
Earl in Module 5
Detailed Netflow CAM (TCAM and ICAM) Utilization
=====
TCAM Utilization   :    0%
ICAM Utilization   :    0%
Netflow TCAM count :    0
Netflow ICAM count :    0
Router#
```

This example shows how to display a summary of the NetFlow table-contention level:

```
Router# show mls netflow table summary
Earl in Module 5
Summary of Netflow CAM Utilization (as a percentage)
=====
TCAM Utilization   :    0%
ICAM Utilization   :    0%
Router#
```

This example shows how to display the NetFlow table-usage notification status:

```
Router# show mls netflow usage
Netflow table usage notification enabled at 80% every 300 seconds
Netflow table utilization of module 7 is 99%
Netflow table utilization of module 40 is 54%
Router#
```

Related Commands	Command	Description
	<a href="#">ip flow-aggregation cache</a>	Creates a flow-aggregation cache and enters the aggregation cache configuration mode.
	<a href="#">mls netflow usage notify</a>	Monitors the NetFlow table usage on the switch processor.
	<a href="#">show ip cache flow</a>	Displays a summary of the NetFlow cache-flow entries.

## show mls netflow ip

To display information about the hardware NetFlow IP, use the **show mls netflow ip** command.

**show mls netflow ip any**

**show mls netflow ip count** [*module number*]

**show mls netflow ip destination** {*hostname* | *ip-address*}[*ip-mask*] [**count** [*module number*]] | **detail** | **dynamic** | **flow** {**icmp** | **tcp** | **udp**} | **module number** / **nowrap** | **qos** | **source** {*hostname* | *ip-address*}[*ip-mask*] | **sw-installed** [**non-static** | **static**]

**show mls netflow ip detail** [*module number* | **nowrap** [*module number*]]

**show mls netflow ip dynamic** [**count** [*module number*]] [**detail**] [*module number*] [**nowrap** [*module number*]] [{**qos** [*module number*] [**nowrap** [*module number*]]}]

**show mls netflow ip** {**flow** {**icmp** | **tcp** | **udp**}} [**count** [*module number*]] {**destination** {*hostname* | *ip-address*}[*ip-mask*]} | **detail** | **dynamic** | **flow** {**icmp** | **tcp** | **udp**} | **module number** / **nowrap** | **qos** | **source** {*hostname* | *ip-address*} | **sw-installed** [**non-static** | **static**]

**show mls netflow ip** {*module number*}

**show mls netflow ip qos** [*module number* | **nowrap** [*module number*]]

**show mls netflow ip source** {*hostname* | *ip-address*}[*ip-mask*] [**count** [*module number*]] | **detail** | **dynamic** | **flow** {**icmp** | **tcp** | **udp**} | **module number** / **nowrap** | **qos** | **sw-installed** [**non-static** | **static**]

### Syntax Description

<b>any</b>	Displays detailed NetFlow table-entry information with no test wrap.
<b>count</b>	Displays the total number of MLS NetFlow IP entries.
<b>module number</b>	(Optional) Displays the entries that are downloaded on the specified module; see the “Usage Guidelines” section for valid values.
<b>destination</b> <i>hostname</i>	Displays the entries for a specific destination hostname.
<b>destination</b> <i>ip-address</i>	Displays the entries for a specific destination IP address.
<i>ip-mask</i>	(Optional) IP mask for a destination IP address.
<b>detail</b>	(Optional) Specifies a detailed output.
<b>dynamic</b>	Displays the hardware-created dynamic entries; see the <a href="#">show mls nde</a> command.
<b>flow icmp</b>	Displays information about the ICMP flows.
<b>flow tcp</b>	Displays information about the TCP flows.
<b>flow udp</b>	Displays information about the UDP flows.
<b>nowrap</b>	Displays information without text wrap.
<b>qos</b>	Displays QoS microflow policing information.
<b>source</b> <i>hostname</i>	Displays the entries for a specific source address.
<b>source</b> <i>ip-address</i>	Displays the entries for a specific source IP address.



## ■ show mls netflow ip

```

QoS Police Count Threshold Leak Drop Bucket Use-Tbl Use-Enable
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
47513014615 47513014515 4 :0 :0 Gi7/4: 0x0
440063 6445898 45 04:45:55 L3 - Dynamic
4 4 0 0 4 0 0 4 4 0 0 0 0
0 0 0 0 0 0 0 0 0 0
0x0 675645504 0 0 NO 34784 NO NO
Router#

```

This example shows how to display NetFlow table-entry information with no test wrap:

```

Router# show mls netflow ip nowrap
Displaying Netflow entries in Supervisor Earl
DstIP SrcIP Prot:SrcPort:DstPort Src i/f
:AdjPtr Pkts Bytes Age LastSeen Attributes
-----
-
-----
45141415 441414195 udp :63 :63 Fa5/44
:0x0 476339 8444594 945 55:34:45 L3 - Dynamic
45141415 441414193 udp :63 :63 Fa5/44
:0x0 476338 8444548 945 55:34:45 L3 - Dynamic
45141415 441414194 udp :63 :63 Fa5/44
:0x0 476338 8444548 945 55:34:45 L3 - Dynamic
45141415 441414195 udp :63 :63 Fa5/44
:0x0 476338 8444548 945 55:34:45 L3 - Dynamic
45141415 441414196 udp :63 :63 Fa5/44
:0x0 476338 8444548 945 55:34:45 L3 - Dynamic
45141415 441414197 udp :63 :63 Fa5/44
:0x0 476337 8444505 945 55:34:45 L3 - Dynamic
45141415 441414198 udp :63 :63 Fa5/44
:0x0 476337 8444505 945 55:34:45 L3 - Dynamic
45141415 441414199 udp :63 :63 Fa5/44
:0x0 476337 8444505 945 55:34:45 L3 - Dynamic
45141415 4414141400 udp :63 :63 Fa5/44
:0x0 476337 8444505 945 55:34:45 L3 - Dynamic
Router#

```

This example shows how to display information about the MLS NetFlow on a specific IP address:

```

Router# show mls netflow ip destination 172.20.52.122
Displaying Netflow entries in Supervisor Earl
DstIP SrcIP Prot:SrcPort:DstPort Src i/f:AdjPtr
-----
Pkts Bytes Age LastSeen Attributes
-----
Router#

```

This example shows how to display information about the MLS NetFlow on a specific flow:

```

Router# show mls netflow ip flow udp
Displaying Netflow entries in Supervisor Earl
DstIP SrcIP Prot:SrcPort:DstPort Src i/f:AdjPtr
-----
Pkts Bytes Age LastSeen Attributes
-----
475150155149 0101010 0 :0 :0 0 : 0
0 0 4407 44:04:35 L3 - Dynamic
Router#

```

This example shows how to display detailed information about the MLS NetFlow on a full-flow mask:

```
Router# show mls netflow ip detail
Displaying Netflow entries in Supervisor Ear1
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts          Bytes          Age  LastSeen  Attributes
-----
      QoS      Police Count Threshold      Leak      Drop Bucket  Use-Tbl Use-Enable
-----+-----+-----+-----+-----+-----+-----+-----+
475150155149      0101010      0 :0      :0      0 : 0
0
      0      4464  44:05:34  L3 - Dynamic
      0x0      0      0      0      NO  64      NO      NO
Router#
```

This example shows how to display detailed information about a specific flow type:

```
Router# show mls netflow ip flow icmp
Displaying Netflow entries in Supervisor Ear1
DstIP SrcIP Prot:SrcPort:DstPort Src i/f
:AdjPtr
>
>-----
-
-
Pkts Bytes Age LastSeen Attributes
-----
45141415 44141401454 icmp:0 :0 Fa5/44
:0x0
4945 89470 4065 08:45:45 L3 - Dynamic
45141415 44141401453 icmp:0 :0 Fa5/44
:0x0
4945 89470 4065 08:45:45 L3 - Dynamic
45141415 44141401455 icmp:0 :0 Fa5/44
:0x0
4945 89470 4065 08:45:45 L3 - Dynamic
45141415 44141401457 icmp:0 :0 Fa5/44
:0x0
4945 89470 4065 08:45:45 L3 - Dynamic
45141415 44141401459 icmp:0 :0 Fa5/44
:0x0
4945 89470 4065 08:45:45 L3 - Dynamic
45141415 44141401464 icmp:0 :0 Fa5/44
:0x0
4945 89470 4065 08:45:45 L3 - Dynamic
45141415 44141401463 icmp:0 :0 Fa5/44
:0x0
Router#
```

## ■ show mls netflow ip

This example shows how to display QoS information:

```
Router# show mls netflow ip qos
Displaying netflow qos information in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts          Bytes          LastSeen   QoS   PoliceCount  Threshold  Leak
-----
Drop  Bucket
-----
xxx1xxxx1xxx1xxx xxx1xxx1xxx1xxx  xxx:63   :63   Fa5/44  :0x0
775357        35558455      47:59:04  xxx   xxx     xxx     xxx
xxx   xxx
Router#
```

## Related Commands

Command	Description
<a href="#">clear mls netflow</a>	Clears the MLS NetFlow-shortcut entries.
<a href="#">ip flow-aggregation cache</a>	Creates a flow-aggregation cache and enters the aggregation cache configuration mode.
<a href="#">show ip cache flow</a>	Displays a summary of the NetFlow cache-flow entries.

# show mls netflow ip sw-installed

To display information for the software-installed IP entries, use the **show mls netflow ip sw-installed** command.

```
show mls netflow ip sw-installed { non-static | static } [count [module number] | detail [module number] | module number]
```

Syntax Description		
<b>non-static</b>	Displays the software-installed routing entries.	
<b>static</b>	Displays the software-installed static routing entries.	
<b>count</b>	(Optional) Displays the total number of nonstatic entries.	
<b>module number</b>	(Optional) Displays the entries that are downloaded on the specified module; see the “Usage Guidelines” section for valid values.	
<b>detail</b>	(Optional) Specifies a detailed per-flow output.	

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the software-installed nonstatic entries:

```
Router> show mls netflow ip sw-installed non-static
Displaying Netflow entries in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts          Bytes          Age  LastSeen  Attributes
-----
Router>
```

This example shows how to display detailed information for the software-installed nonstatic entries:

```
Router> show mls netflow ip sw-installed non-static detail
Displaying Netflow entries in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts          Bytes          Age  LastSeen  Attributes
-----
QoS          Police Count Threshold  Leak  Drop Bucket  Use-Tbl Use-Enable
-----+-----+-----+-----+-----+-----+-----+
Router>
```

This example shows how to display the total number of software-installed nonstatic entries:

```
Router> show mls netflow ip sw-installed non-static count
Displaying Netflow entries in Supervisor Earl

Number of shortcuts = 0
Router>
```

## show mls netflow ipv6

To display information about the hardware NetFlow IPv6 configuration, use the **show mls netflow ipv6** command.

**show mls netflow ipv6 any**

**show mls netflow ipv6 count** [*module number*]

**show mls netflow ipv6 destination** *ipv6-address*[*ipv6-prefix*] [**count** [*module number*]] | **detail** | **dynamic** | **flow** {**icmp** | **tcp** | **udp**} | **module number** / **nowrap** | **qos** | **source** *ipv6-address*[*ipv6-prefix*] | **sw-installed** [**non-static** | **static**]

**show mls netflow ipv6 detail** [*module number* | **nowrap** [*module number*]]

**show mls netflow ipv6 dynamic** [**count** [*module number*]] [**detail**] [*module number*] [**nowrap** [*module number*]] [{**qos** [*module number*]}] [**nowrap** [*module number*]]

**show mls netflow ipv6** {**flow** {**icmp** | **tcp** | **udp**}} [**count** [*module number*]] | {**destination** *ipv6-address*[*ipv6-prefix*]} | **detail** | **dynamic** | **flow** {**icmp** | **tcp** | **udp**} | **module number** / **nowrap** | **qos** | {**source** *ipv6-address*[*ipv6-prefix*]} | **sw-installed** [**non-static** | **static**]

**show mls netflow ipv6** {*module number*}

**show mls netflow ipv6 qos** [*module number* | **nowrap** [*module number*]]

**show mls netflow ipv6 source** *ipv6-address*[*ipv6-prefix*] [**count** [*module number*]] | **detail** | **dynamic** | **flow** {**icmp** | **tcp** | **udp**} | **module number** / **nowrap** | **qos** | **sw-installed** [**non-static** | **static**]

### Syntax Description

<b>any</b>	Displays the NetFlow-aging information.
<b>count</b>	Displays the total number of MLS NetFlow IPv6 entries.
<b>module number</b>	(Optional) Displays the entries that are downloaded on the specified module; see the “Usage Guidelines” section for valid values.
<b>destination</b> <i>ipv6-address</i> <i>ipv6-prefix</i>	Displays the entries for a specific destination IPv6 address. IPv6 prefix; valid values are from 0 to 128.
<b>detail</b>	Specifies a detailed output.
<b>dynamic</b>	Displays the hardware-created dynamic entries.
<b>flow</b> <b>icmp</b>   <b>tcp</b>   <b>udp</b>	Specifies the flow type.
<b>nowrap</b>	(Optional) Turns off text wrapping.
<b>qos</b>	Displays information about QoS statistics.
<b>source</b> <i>ipv6-address</i>	(Optional) Displays the entries for a specific source IPv6 address.
<b>sw-installed</b>	(Optional) Displays the routing NetFlow entries.
<b>non-static</b>	(Optional) Displays information about the software-installed static IPv6 entries.
<b>static</b>	(Optional) Displays information about the software-installed nonstatic IPv6 entries.

## ■ show mls netflow ipv6

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display information about the hardware NetFlow configuration:

```
Router# show mls netflow ipv6
Displaying Netflow entries in Supervisor Earl
DstIP                               SrcIP
-----
Prot:SrcPort:DstPort  Src i/f      :AdjPtr
Pkts      Bytes      Age  LastSeen  Attributes
-----
50::5
tcp :46      :35      V147      :0x0
53758      4455480   4    53:48:36  L3 (IPv6) - Dynamic
50::5
tcp :46      :35      V147      :0x0
53758      4455480   4    53:48:36  L3 (IPv6) - Dynamic
50::5
tcp :46      :35      V147      :0x0
53758      4455480   4    53:48:36  L3 (IPv6) - Dynamic
50::5
tcp :46      :35      V147      :0x0
53758      4455480   4    53:48:36  L3 (IPv6) - Dynamic
50::5
tcp :46      :35      V147      :0x0
53758      4455480   4    53:48:36  L3 (IPv6) - Dynamic
50::5
tcp :46      :35      V147      :0x0
53758      4455480   4    53:48:36  L3 (IPv6) - Dynamic
Router#
```

This example shows how to display IPv6 microflow policing information:

```
Router# show mls netflow ipv6 qos
Displaying Netflow entries in Supervisor Earl
DstIP                               SrcIP
-----
Prot:SrcPort:DstPort  Src i/f      :AdjPtr  Pkts      Bytes
-----
LastSeen  QoS      PoliceCount  Threshold  Leak      Drop  Bucket
-----
404::3
icmp:0      :0      --          0x0
55:55:09   0x0     0           0           0         NO    0
404::5
icmp:0      :0      --          0x0
55:55:09   0x0     0           0           0         NO    0
Router#
```

This example shows how to display IPv6 microflow policing information for a specific module:

```
Router# show mls netflow ipv6 qos module 7
Displaying Netflow entries in module 7
DstIP                               SrcIP
-----
Prot:SrcPort:DstPort  Src i/f          :AdjPtr  Pkts      Bytes
-----
LastSeen  QoS    PoliceCount  Threshold  Leak      Drop  Bucket
-----
404::5
icmp:0    :0      --          0x0        0         0      0
55:55:56  0x0    0           0           0         NO    0
404::3
icmp:0    :0      --          0x0        0         0      0
55:55:56  0x0    0           0           0         NO    0
Router#
```

This example shows the output display when you turn off text wrapping:

```
Router# show mls netflow ipv6 qos nowrap
Displaying Netflow entries in Supervisor Earl
DstIP                               SrcIP
Prot:SrcPort:DstPort  Src i/f          :AdjPtr  Pkts      Bytes      LastSeen
QoS    PoliceCount  Threshold  Leak      Drop  Bucket
-----
-----
404::3
:0      --          0x0        0         0         55:55:49  0x0    0      icmp:0
0       0          NO    0
404::5
:0      --          0x0        0         0         55:55:49  0x0    0      icmp:0
0       0          NO    0
Router#
```

This example shows the output display when you turn off text wrapping for a specific module:

```
Router# show mls netflow ipv6 qos nowrap module 7
Displaying Netflow entries in module 7
DstIP                               SrcIP
Prot:SrcPort:DstPort  Src i/f          :AdjPtr  Pkts      Bytes      LastSeen
QoS    PoliceCount  Threshold  Leak      Drop  Bucket
-----
-----
404::3
:0      --          0x0        0         0         55:55:38  0x0    0      icmp:0
0       0          NO    0
404::5
:0      --          0x0        0         0         55:55:38  0x0    0      icmp:0
0       0          NO    0
Router#
```

#### Related Commands

Command	Description
<a href="#">clear mls netflow</a>	Clears the MLS NetFlow-shortcut entries.

# show mls qos

To display MLS QoS information, use the **show mls qos** command.

```
show mls qos [{arp | ipv6 | ip | ipx | last | mac | maps [map-type]} [{interface interface-number}
| {slot slot} | {null interface-number} | {port-channel number} | {vlan vlan-id}]]
```

Syntax Description	
<b>arp</b>	(Optional) Displays ARP information.
<b>ipv6</b>	(Optional) Displays IPv6 information.
<b>ip   ipx</b>	(Optional) Displays information about the MLS IP or IPX status.
<b>last</b>	(Optional) Displays information about the last packet-policing.
<b>mac</b>	(Optional) Displays information about the MAC address-based QoS status.
<b>maps</b>	(Optional) Displays information about the QoS mapping.
<i>map-type</i>	(Optional) Map type; see the “Usage Guidelines” section for valid values.
<i>interface</i>	(Optional) Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>ge-wan</b> , <b>pos</b> , and <b>atm</b> .
<i>interface-number</i>	(Optional) Module and port number; see the “Usage Guidelines” section for valid values.
<b>slot slot</b>	(Optional) Specifies the slot number; displays the global and per-interface QoS enabled and disabled settings and the global QoS counters.
<b>null interface-number</b>	(Optional) Specifies the null interface; the valid value is <b>0</b> .
<b>port-channel number</b>	(Optional) Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 282.
<b>vlan vlan-id</b>	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The **port-channel number** values from 257 to 282 are supported on the CSM and the FWSM only.

Valid values for *map-types* are defined as follows:

- **cos-dscp**—Specifies the ingress CoS-to-DSCP mapping to display; valid values are from 0 to 7.
- **dscp-cos**—Displays the egress DSCP-to-CoS mapping.
- **dscp-exp**—Displays the DSCP-to-EXP mapping on the MPLS domain ingress and egress; this keyword is not supported.
- **exp-dscp**—Displays the EXP-to-DSCP mapping on the MPLS domain ingress and egress; this keyword is not supported.
- **ip-prec-dscp value**—Specifies the ingress IP precedence-to-DSCP mapping to display; valid values are from 0 to 7.
- **policed-dscp**—Displays the policed DSCP values to marked-down DSCP values mapping.

The **dscp-exp** and **exp-dscp** options are supported on Catalyst 6500 series switches that are configured with a Supervisor Engine 720 only.

## Examples

This example shows how to display information about the last logged packet:

```
Router# show mls qos last
QoS engine last packet information:
  Packet was transmitted
  Output TOS/DSCP: 0xC0/48 [unchanged]   Output COS: 0 [unchanged]
  Aggregate policer index: 0 (none)
  Microflow policer index: 0 (none)
Router#
```

This example shows how to display the QoS-map settings:

```
Router# show mls qos maps
Policed-dscp map:
  0  4  5  3  4  5  6  7  8  9
-----
00:  00 04 05 03 04 05 06 07 08 09
40:  40 44 45 43 44 45 46 47 48 49
50:  50 54 55 53 54 55 56 57 58 59
30:  30 34 35 33 34 35 36 37 38 39
40:  40 44 45 43 44 45 46 47 48 49
50:  50 54 55 53 54 55 56 57 58 59
60:  60 64 65 63

Dscp-cos map:
  0  4  5  3  4  5  6  7  8  9
-----
00:  00 00 00 00 00 00 00 00 04 04
40:  04 04 04 04 04 04 05 05 05 05
50:  05 05 05 05 03 03 03 03 03 03
30:  03 03 04 04 04 04 04 04 04 04
40:  05 05 05 05 05 05 05 05 06 06
50:  06 06 06 06 06 06 07 07 07 07
60:  07 07 07 07

Cos-dscp map:
  cos:  0  4  5  3  4  5  6  7
-----
  dscp:  0  8 46 54 35 40 48 56

IpPrecedence-dscp map:
  ipprec:  0  4  5  3  4  5  6  7
-----
```

```
dscp: 0 8 46 54 35 40 48 56
```

```
Router#
```

This example shows how to verify the configuration of DSCP-mutation mapping:

```
Router# show mls qos maps | begin DSCP mutation
DSCP mutation map mutmap4: (dscp= d4d5)
  d4 : d5 0 4 5 3 4 5 6 7 8 9
-----
  0 : 00 04 05 03 04 05 06 07 08 09
  4 : 40 44 45 43 44 45 46 47 48 49
  5 : 50 54 55 53 54 55 56 57 58 59
  3 : 08 34 35 33 34 35 36 37 38 39
  4 : 40 44 45 43 44 45 46 47 48 49
  5 : 50 54 55 53 54 55 56 57 58 59
  6 : 60 64 65 63
<111Output Truncated111>
Router#
```



#### Note

In the DSCP-mutation map displays, the marked-down DSCP values are shown in the body of the matrix. The first digit of the original DSCP value is in the column labeled d1, and the second digit is in the top row. In the example, DSCP 30 maps to DSCP 08.

This example shows how to display IPv6 information:

```
Router# show mls qos ipv6
QoS Summary [IPv6]: (* - shared aggregates, Mod - switch module)

  Int Mod Dir  Class-map DSCP  Agg  Trust Fl  AgForward-By  AgPoliced-By
                Id      Id      Id
-----
  All 7  -   Default  0    0*   No  0    489445356    0
Router#
```

This example shows how to display QoS information:

```
Router# show mls qos
QoS is enabled globally
Microflow policing is enabled globally
QoS ip packet dscp rewrite enabled globally

QoS is disabled on the following interfaces:
Fa6/3 Fa6/4

QoS DSCP-mutation map is enabled on the following interfaces:
Fa6/5
Vlan or Portchannel(Multi-Earl) policies supported: \es
Egress policies supported: \es

----- Module [5] -----
QoS global counters:
Total packets: 464
IP shortcut packets: 0
Packets dropped by policing: 0
IP packets with TOS changed by policing: 0
IP packets with COS changed by policing: 0
Non-IP packets with COS changed by policing: 0
MPLS packets with EXP changed by policing: 0
Router#
```

Related Commands	Command	Description
	<b>mls qos (global configuration mode)</b>	Enables the QoS functionality globally.
	<b>mls qos (interface configuration mode)</b>	Enables the QoS functionality on an interface.

# show mls qos free-agram

To display the number of free aggregate RAM indexes on the switch processor, use the **show mls qos free-agram** command.

**show mls qos free-agram**

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

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the number of free aggregate RAM indexes on the switch processor :

```
Router# show mls qos free-agram
Total Number of Available AG RAM indices : 4053

Module [4]
Free AGIDs : 4053

Module [6]
Free AGIDs : 4053

Router#
```

# show mls qos maps

To display information about the QoS-map configuration and runtime-version, use the **show mls qos maps** command.

```
show mls qos maps [cos-dscp | cos-mutation | dscp-cos | dscp-exp | dscp-mutation | exp-dscp |
exp-mutation | ip-prec-dscp | policed-dscp]
```

Syntax Description	
<b>cos-dscp</b>	(Optional) Displays information about the CoS-to-DSCP map.
<b>cos-mutation</b>	(Optional) Displays information about the CoS-mutation map.
<b>dscp-cos</b>	(Optional) Displays information about the DSCP-to-CoS map.
<b>dscp-exp</b>	(Optional) Displays information about the DSCP-to-exp map.
<b>dscp-mutation</b>	(Optional) Displays information about the DSCP-mutation map.
<b>exp-dscp</b>	(Optional) Displays information about the exp-to-DSCP map.
<b>exp-mutation</b>	(Optional) Displays information about the exp-mutation map.
<b>ip-prec-dscp</b>	(Optional) Displays information about the IP precedence-to-DSCP map.
<b>policed-dscp</b>	(Optional) Displays information about the policed-DSCP map.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display information about the QoS-map configuration and runtime version:

```
Router# show mls qos maps
Normal Burst Policed-dscp map: (dscp= d4d5)
d4 : d5 0 4 5 3 4 5 6 7 8 9
-----
0 : 00 04 05 03 04 05 06 07 08 09
4 : 40 44 45 43 44 45 46 47 48 49
5 : 50 54 55 53 54 55 56 57 58 59
3 : 30 34 35 33 34 35 36 37 38 39
4 : 40 44 45 43 44 45 46 47 48 49
5 : 50 54 55 53 54 55 56 57 58 59
6 : 60 64 65 63

Maximum Burst Policed-dscp map: (dscp= d4d5)
d4 : d5 0 4 5 3 4 5 6 7 8 9
-----
0 : 00 04 05 03 04 05 06 07 08 09
4 : 40 44 45 43 44 45 46 47 48 49
5 : 50 54 55 53 54 55 56 57 58 59
3 : 30 34 35 33 34 35 36 37 38 39
```

## ■ show mls qos maps

```

4 :    40 44 45 43 44 45 46 47 48 49
5 :    50 54 55 53 54 55 56 57 58 59
6 :    60 64 65 63

```

```
Dscp-cos map: (dscp= d4d5)
```

```

d4 : d5 0  4  5  3  4  5  6  7  8  9
-----
0 :    00 00 00 00 00 00 00 00 04 04
4 :    04 04 04 04 04 04 05 05 05 05
5 :    05 05 05 05 03 03 03 03 03 03
3 :    03 03 04 04 04 04 04 04 04 04
4 :    05 05 05 05 05 05 05 05 06 06
5 :    06 06 06 06 06 06 07 07 07 07
6 :    07 07 07 07

```

```
Cos-dscp map:
```

```

cos:   0  4  5  3  4  5  6  7
-----
dscp:  0  8 46 54 35 40 48 56

```

```
IpPrecedence-dscp map:
```

```

ipprec:  0  4  5  3  4  5  6  7
-----
dscp:   0  8 46 54 35 40 48 56

```

```
Router#
```

This example shows how to display the configuration and runtime version of the CoS-to-CoS map:

```
Router# show mls qos maps cos-mutation
```

```
CoS mutation map test-map:
```

```
In-CoS : Out-CoS
```

```

-----
0 :      0
4 :      4
5 :      5
3 :      4
4 :      4
5 :      4
6 :      6
7 :      7

```

```
Router#
```

## Related Commands

Command	Description
<a href="#">mls qos map cos-dscp</a>	Defines the ingress CoS-to-DSCP map for trusted interfaces.
<a href="#">mls qos map cos-mutation</a>	Maps a packet's CoS to a new CoS value.
<a href="#">mls qos map dscp-cos</a>	Defines an egress DSCP-to-CoS map.
<a href="#">mls qos map dscp-mutation</a>	Defines a named DSCP mutation map.
<a href="#">mls qos map ip-prec-dscp</a>	Defines an ingress-IP precedence-to-DSCP map for trusted interfaces.
<a href="#">mls qos map policed-dscp</a>	Sets the mapping of policed DSCP values to marked-down DSCP values.

# show mls qos mpls

To display an interface summary for MPLS QoS classes in the policy maps, use the **show mls qos mpls** command.

```
show mls qos mpls [{interface interface-number} | {module slot}]
```

Syntax Description		
<i>interface</i>	(Optional) Interface type; possible valid values are <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> .	
<i>interface-number</i>	Module and port number; see the “Usage Guidelines” section for valid values.	
<b>module slot</b>	(Optional) Specifies the module slot number.	

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command is supported in PFC3BXL or PFC3B mode only.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

**Examples** This example shows how to display an interface summary for MPLS QoS classes in the policy maps:

```
Router# show mls qos mpls
QoS Summary [MPLS]: (* - shared aggregates, Mod - switch module)
Int Mod Dir Class-map DSCP Agg Trust Fl AgForward-By AgPoliced-By
Id Id
-----
-----
Fa3/38 5 In exp5 0 4 dscp 0 378900 0
Fa3/44 5 In exp4 0 3 dscp 0 0 0
All 5 - Default 0 0* No 0 4494044540 0
Router#
```

■ show mls qos mpls

---

**Related Commands**

Command	Description
<a href="#">mls qos exp-mutation</a>	Attaches an egress-EXP mutation map to the interface.
<a href="#">mls qos map exp-dscp</a>	Defines the ingress EXP value to the internal DSCP map.
<a href="#">mls qos map exp-mutation</a>	Maps a packet's EXP to a new EXP value.

---

# show mls qos protocol

To display protocol pass-through information, use the **show mls qos protocol** command.

**show mls qos protocol** [*module num*]

<b>Syntax Description</b>	<b>module num</b> (Optional) Specifies the module number.
---------------------------	---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display protocol pass-through information:

```
Router# show mls qos protocol
RIP : Passthru mode
OSPF : Passthru mode
ND : Policing mode Cir = 35000 Burst = 4000
----- Module [5] -----
Routing protocol RIP is using AgId 0*
Routing protocol OSPF is using AgId 0*
Routing protocol ND is using AgId 4
----- Module [6] -----
Routing protocol RIP is using AgId 0*
Routing protocol OSPF is using AgId 0*
Router#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">mls qos protocol</a>	Defines the routing-protocol packet policing.

# show mls qos statistics-export info

To display information about the MLS-statistics data-export status and configuration, use the **show mls qos statistics-export info** command.

## show mls qos statistics-export info

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

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display information about the MLS-statistics data-export status and configuration:

```
Router# show mls qos statistics-export info
QoS Statistics Data Export Status and Configuration information
-----
Export Status : enabled
Export Interval : 550 seconds
Export Delimiter : @
Export Destination : 47515015513, UDP port 544 Facility local6, Severity debug

QoS Statistics Data Export is enabled on following ports:
-----
FastEthernet5/54

QoS Statistics Data export is enabled on following shared aggregate policers:
-----
aggr4M

QoS Statistics Data Export is enabled on following class-maps:
-----
class3
Router#
```

Related Commands	Command	Description
	<b>mls qos statistics-export (global configuration mode)</b>	Enables QoS-statistics data export globally.
	<b>mls qos statistics-export (interface configuration mode)</b>	Enables per-port QoS-statistics data export.
	<b>mls qos statistics-export aggregate-policer</b>	Enables QoS-statistics data export on the named aggregate policer.
	<b>mls qos statistics-export class-map</b>	Enables QoS-statistics data export for a class map.
	<b>mls qos statistics-export delimiter</b>	Sets the QoS-statistics data-export field delimiter.
	<b>mls qos statistics-export destination</b>	Configures the QoS-statistics data-export destination host and UDP port number.
	<b>mls qos statistics-export interval</b>	Specifies how often a port and/or aggregate-policer QoS-statistics data is read and exported.

## show mls rate-limit

To display information about the MLS rate limiter, use the **show mls rate-limit** command.

**show mls rate-limit [usage]**

<b>Syntax Description</b>	<b>usage</b> (Optional) Displays the feature that is used with the rate-limiter register.
---------------------------	---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

In the command output, the rate-limit status could be one of the following:

- On indicates a rate for that particular case has been set.
- Off indicates that the rate-limiter type has not been configured, and the packets for that case are not rate limited.
- On/Sharing indicates a particular case (not manually configured) is affected by the configuration of another rate limiter belonging to the same sharing group.
- A hyphen indicates that the multicast partial-SC rate limiter is disabled.

In the command output, the rate-limit sharing indicates the following information:

- Whether sharing is static or dynamic
- Group dynamic sharing codes

The **show mls rate-limit usage** command displays the hardware register that is used by a rate-limiter type. If the register is not used by any rate-limiter type, Free is displayed in the output. If the register is used by a rate-limiter type, Used and the rate-limiter type are displayed.

**Examples**

This example shows how to display information about the rate-limit status:

```
Router# show mls rate-limit
Sharing Codes: S - static, D - dynamic
Codes dynamic sharing: H - owner (head) of the group, g - guest of the group
```

Rate Limiter Type	Status	Packets/s	Burst	Sharing
MCAST NON RPF	Off	-	-	-
MCAST DFLT ADJ	On	400000	400	Not sharing
MCAST DIRECT CON	Off	-	-	-
ACL BRIDGED IN	Off	-	-	-
ACL BRIDGED OUT	Off	-	-	-

```

IP FEATURES Off - -
ACL VACL LOG On 5000 4 Not sharing
CEF RECEIVE Off - -
CEF GLEAN Off - -
MCAST PARTIAL SC On 400000 400 Not sharing
IP RPF FAILURE On 400 40 Group:0 S
TTL FAILURE On 4000 40 Not sharing
ICMP UNREAC1 NO-ROUTE On 400 40 Group:0 S
ICMP UNREAC1 ACL-DROP On 400 40 Group:0 S
ICMP REDIRECT Off - -
MTU FAILURE On 4000 400 Not sharing
MCAST IP OPTION Off - -
UCAST IP OPTION Off - -
LA\ER_5 PDU Off - -
LA\ER_5 PT Off - -
LA\ER_5 PORTSEC On 40000 4 Not sharing
IP ERRORS On 400 40 Group:0 S
CAPTURE PKT Off - -
MCAST IGMP Off - -
MCAST IPv6 DIRECT CON Off - -
MCAST IPv6 ROUTE CNTL Off - -
MCAST IPv6 *G M BRIDG Off - -
MCAST IPv6 SG BRIDGE Off - -
MCAST IPv6 DFLT DROP Off - -
MCAST IPv6 SECOND1 DR Off - -
MCAST IPv6 *G BRIDGE Off - -
MCAST IPv6 MLD Off - -
IP ADMIS1 ON L5 PORT Off - -
Router#

```

This example shows how to display information about the rate-limit usage:

```

Router# show mls rate-limit usage
Rate Limiter Type      Packets/s  Burst
-----
Layer3 Rate Limiters:
RL# 0: Free            -          -
RL# 4: Free            -          -
RL# 5: Free            -          -
RL# 3: Used
MCAST DFLT ADJ        400000    400
RL# 4: Used
MTU FAILURE           4000     400
RL# 5: Used
TTL FAILURE           4000     400
RL# 6: Used
IP RPF FAILURE         400      40
ICMP UNREAC1 NO-ROUTE 400      40
ICMP UNREAC1 ACL-DROP 400      40
IP ERRORS              400      40
RL# 7: Used
ACL VACL LOG          5000     4
RL# 8: Rsvd for capture -          -

Layer5 Rate Limiters:
RL# 9: Reserved
RL#40: Reserved
RL#44: Free            -          -
RL#45: Used
LA\ER_5 PORTSEC       40000    4

Router #

```

■ show mls rate-limit

Related Commands	Command	Description
	<a href="#">mls rate-limit layer2</a>	Enables and sets the rate limiters for the control packets in Layer 2.
	<a href="#">mls rate-limit multicast ipv4</a>	Enables and sets the rate limiters for the IPv4 multicast packets.
	<a href="#">mls rate-limit multicast ipv6</a>	Configures the IPv6 multicast rate limiters.
	<a href="#">mls rate-limit unicast acl</a>	Enables and sets the ACL-bridged rate limiters.

# show mls sampling

To display information about the sampled NDE status, use the **show mls sampling** command.

## show mls sampling

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

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Sampled NetFlow is supported on Layer 3 interfaces only.

**Examples** This example shows how to display information about the sampled NDE status:

```
Router# show mls sampling
time-based sampling is enabled
4 out of every 4054 packets is being sampled1
Sampling Interval and Period is 4 millisec per 4096 millisec
Router#
```

Related Commands	Command	Description
	<a href="#">mls netflow sampling</a>	Enables the sampled NetFlow on an interface.
	<a href="#">mls sampling</a>	Enables the sampled NetFlow and specifies the sampling method.

## show mls statistics

To display the MLS statistics for the IP, multicast, Layer 2 protocol, and QoS, use the **show mls statistics** command.

**show mls statistics** [*module num* | *protocol type*]

Syntax Description	module num	(Optional) Displays the MLS statistics for a specific module.
	protocol type	(Optional) Displays MLS statistics information based on a protocol (such as Telnet, FTP, or WWW).

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The total packets switched performance displayed is the rate calculated as the average rate in a period within the last 30 seconds.

The ingress ACL denied packet count is displayed in the Total packets L3 Switched field and in the Total packets dropped by ACL field.

The RPF failed packet count is displayed in the Total packets L3 Switched field.

If the IP multicast source sends traffic to any multicast group that does not have an (\*,G) entry present in the mroute table, the **show mls statistics** command displays these packets as incrementing in the Total Mcast Packets Switched/Routed field. These packets are dropped in the hardware because there are no receivers for that group and no entry in the mroute table.

**Examples** This example shows how to display the MLS statistics for all modules:

```
Router# show mls statistics

Statistics for Earl in Module 5

L5 Forwarding Engine
  Total packets Switched           : 50573@ 55555 pps

L3 Forwarding Engine
  Total Packets Bridged             : 50573
  Total Packets FIB Switched        : 7864
  Total Packets ACL Routed          : 0
  Total Packets Netflow Switched    : 0
  Total Mcast Packets Switched/Routed : 550598
  Total ip packets with TOS changed : 0
```

```

Total ip packets with COS changed      : 0
Total non ip packets COS changed      : 0
Total packets dropped by ACL          : 0
Total packets dropped by Policing     : 705757744

Statistics for Earl in Module 9

L5 Forwarding Engine
  Total packets Switched               : 46683@ 4 pps

L3 Forwarding Engine
  Total Packets Bridged                : 0
  Total Packets FIB Switched           : 0
  Total Packets ACL Routed             : 0
  Total Packets Netflow Switched      : 0
  Total Mcast Packets Switched/Routed  : 0
  Total ip packets with TOS changed    : 0
  Total ip packets with COS changed    : 0
  Total non ip packets COS changed     : 0
  Total packets dropped by ACL         : 0
  Total packets dropped by Policing    : 577949053
Router#

```

This example shows how to display the MLS statistics for a specific module:

```

Router# show mls statistics module 1

Statistics for Earl in Module 4

L5 Forwarding Engine
  Total packets Switched               : 5748466@ 55335 pps
>>
L3 Forwarding Engine
  Total Packets Bridged                : 95750@ 34 pps
  Total Packets FIB Switched           : 7
  Total Packets ACL Routed             : 0
  Total Packets Netflow Switched      : 0
  Total Mcast Packets Switched/Routed  : 3079500
  Total ip packets with TOS changed    : 0
  Total ip packets with COS changed    : 0
  Total non ip packets COS changed     : 0
  Total packets dropped by ACL         : 0
  Total packets dropped by Policing    : 0
  Total Unicast RPF failed packets     : 0

Errors
  MAC/IP length inconsistencies       : 0
  Short IP packets received           : 0
  IP header checksum errors           : 0
  MAC/IPX length inconsistencies     : 0
  Short IPX packets received          : 0
Router#

```

# show mls table-contention

To display TCL information, use the **show mls table-contention** command.

**show mls table-contention** { **detailed** | **summary** | **aggregate** }

Syntax Description		
	<b>detailed</b>	Displays the detailed TCL information.
	<b>summary</b>	Displays the TCL level.
	<b>aggregate</b>	Displays the aggregate count of all missed flows in the Supervisor Engine 720 and page hits/misses in Supervisor Engine 2.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** You can enter the **aggregate** keyword to display the statistics for the NetFlow-creation failures and NetFlow-hash aliases in the Supervisor Engine 720.

You can enter the **aggregate** keyword to display the page hits and misses in the Supervisor Engine 2.

The last reading of the corresponding registers are displayed in the **summary** and **detailed** keywords for the Supervisor Engine 720.

**Examples** This example shows how to display a detailed list of TCL information:

```
Router# show mls table-contention detailed
Detailed Table Contention Level Information
=====
Layer 3
-----
L3 Contention Level:      0
Page Hits Requiring 4 Lookup   =      34
Page Hits Requiring 5 Lookups  =       0
Page Hits Requiring 3 Lookups  =       0
Page Hits Requiring 4 Lookups  =       0
Page Hits Requiring 5 Lookups  =       0
Page Hits Requiring 6 Lookups  =       0
Page Hits Requiring 7 Lookups  =       0
Page Hits Requiring 8 Lookups  =       0
Page Misses                   =       0
Router#
```

This example shows how to display a summary of TCL information:

```
Router# show mls table-contention summary
```

```
Summary of Table Contention Levels (on a scale of 0 (lowest) to 3 (highest))
=====
L3 Contention Level: 0
```

This example shows how to display an aggregate count of all missed flows in the Supervisor Engine 720 and page hits/misses in Supervisor Engine 2:

```
Router# show mls table-contention aggregate
Earl in Module 4
Detailed Table Contention Level Information
=====
Layer 3
-----
L3 Contention Level:      0
Page Hits Requiring 4 Lookup   =      54000
Page Hits Requiring 5 Lookups  =       480
Page Hits Requiring 3 Lookups  =        0
Page Hits Requiring 4 Lookups  =        0
Page Hits Requiring 5 Lookups  =        0
Page Hits Requiring 6 Lookups  =        0
Page Hits Requiring 7 Lookups  =        0
Page Hits Requiring 8 Lookups  =        0
Page Misses                   =        0
```

# show mmls igmp explicit-tracking

To display information about the host-tracking database, use the **show mmls igmp explicit-tracking** command.

**show mmls igmp explicit-tracking** [*vlan-id*]

<b>Syntax Description</b>	<i>vlan-id</i> (Optional) VLAN ID; valid values are 1 to 4094.
---------------------------	--

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

<b>Command Modes</b>	Switch processor—Privileged EXEC
----------------------	----------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display information about the host-tracking database for a specific VLAN:

```
Switch-sp# show mmls igmp explicit-tracking 27
```

Source/Group	Interface	Reporter	Filter_mode
40141414/554141414	V157:3/55	461571513	INCLUDE
40151515/554141414	V157:3/55	461571513	INCLUDE

```
Router#
```

# show mmls msc

To display information about MMLS, use the **show mmls msc** command.

**show mmls msc** [**cache** | **entry** | **icroif-cache** | **rpdf-cache** | **statistics** | **vpn**]

Syntax Description		
<b>cache</b>	(Optional)	Displays information about the multicast shortcuts for the process cache.
<b>entry</b>	(Optional)	Displays information about the dump-hardware entries in Layer 3.
<b>icroif-cache</b>	(Optional)	Displays information about the dump-ICROIF cache.
<b>rpdf-cache</b>	(Optional)	Displays information about the dump-Bidir RPDF cache.
<b>statistics</b>	(Optional)	Displays statistics about the multicast-shortcuts process.
<b>vpn</b>	(Optional)	Displays information about VPN.

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

**Command Modes** Switch processor—Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display information about MMLS:

Switch-sp# **show mmls msc**

```

General Info
-----+-----+
Number shortcuts in software database          4890
Number of MFD in software database            4890
Router MAC                                     0004164f814b00
Internal Vlan                                  4093
Aggregation Vlan                              0
Aggregation Indexes                           0
Current Size of inputQ                         0
Maximum Size of inputQ                         5
flow statistics timeout [sec]                  55
non-rpf MFDs purge timeout [sec]              50
non-rpf MFDs aging timeout [sec]              510
Switch-sp#

```

This example shows how to display information about the MMLS shortcut-process cache:

Switch-sp# **show mmls msc cache**

```

-----macg cache buckets for vpn 0-----
Bucket 90 #g: 4
Group mac address: 040015e0410405
$$$ (S,G,C): (400101014, 554141415, 400)      mfd_flag: 4  type: Sparse

```

```

$$$ (S,G,C): (0101010, 554141415, 4)      mfd_flag: 4  type: Sparse
### vlan: 400  sc_count: 0 rpf_count: 4
### vlan: 4    sc_count: 0 rpf_count: 4
Bucket 94 #g: 4
Group mac address: 040015e0410404
$$$ (S,G,C): (400101014, 554141414, 400)  mfd_flag: 4  type: Sparse
$$$ (S,G,C): (0101010, 554141414, 4)      mfd_flag: 4  type: Sparse
### vlan: 400  sc_count: 0 rpf_count: 4
### vlan: 4    sc_count: 0 rpf_count: 4
Bucket 95 #g: 4
Group mac address: 040015e0410403
$$$ (S,G,C): (400101014, 554141413, 400)  mfd_flag: 4  type: Sparse
$$$ (S,G,C): (0101010, 554141413, 4)      mfd_flag: 4  type: Sparse
### vlan: 400  sc_count: 0 rpf_count: 4
### vlan: 4    sc_count: 0 rpf_count: 4
Bucket 93 #g: 4
Group mac address: 040015e0410405
$$$ (S,G,C): (400101014, 554141415, 400)  mfd_flag: 4  type: Sparse
$$$ (S,G,C): (0101010, 554141415, 4)      mfd_flag: 4  type: Sparse
### vlan: 400  sc_count: 0 rpf_count: 4
### vlan: 4    sc_count: 0 rpf_count: 4
Bucket 94 #g: 4
Group mac address: 040015e0410404
$$$ (S,G,C): (400101014, 554141414, 400)  mfd_flag: 4  type: Sparse
$$$ (S,G,C): (0101010, 554141414, 4)      mfd_flag: 4  type: Sparse
### vlan: 400  sc_count: 0 rpf_count: 4
### vlan: 4    sc_count: 0 rpf_count: 4
Switch-sp#

```

This example shows how to display dump ICROIF-cache information:

```

Switch-sp# show mmls msc icroif-cache

mmls_local_icroif_index: 0x493
mmls_global_icroif_index: 0x494

ICROIF CACHE:
-----
Module mask: 0x8      Icroif_index: 0x495
Switch-sp#

```

This example shows how to display a dump list of DF interfaces for the PIM-RPs:

```

Switch-sp# show mmls msc rpdf-cache

----- RP-CACHE [VPN-0] -----

Bucket# :0

RP-addr: 4101014, Rpf: 0 Vpn: 0
DF-index: 0
DF-list: 504 505 503 504 505 506 507 508 509 540
        544 545
Group-list:
          (554141010/54, H)
G/m-count: 4, G/35-count: 4

Bucket# :5

RP-addr: 3101014, Rpf: 0 Vpn: 0
DF-index: 5
DF-list: 504 505 503 504 505 506 507 508 509 540
        544 545

```

```

Group-list:
  (554141510/54, H)
G/m-count: 4, G/35-count: 0

Bucket# :3

RP-addr: 5101014, Rpf: 0 Vpn: 0
DF-index: 4
DF-list: 504 505 503 504 505 506 507 508 509 540
         544 545
Group-list:
  (554141410/54, H)
G/m-count: 4, G/35-count: 4

Bucket# :5

RP-addr: 4101014, Rpf: 0 Vpn: 0
DF-index: 3
DF-list: 504 505 503 504 505 506 507 508 509 540
         544 545
Group-list:
  (554141310/54, H)
G/m-count: 4, G/35-count: 0

Switch-sp#

```

This example shows how to display the statistics for the multicast-shortcut process:

```
Switch-sp# show mmls msc statistics
```

```

Communication Statistics
-----+-----+
Number MSM PDU Received           4
Number MSM PDU Sent                4
Unsolicited Feature Notification Sent 4
Feature Notification Received      5
Feature Notification Sent          5
Stop retry Sent                    0
Stop download Sent                 0

Error Statistics
-----+-----+
L5 entry not found                 0
LTL full error                     0
MET full error                     0

Debug Statistics
-----+-----+
HW Met failure                     0
HW Dist failure                    0
HW L3 Install failure              0
HW L3 Update failure               0

TLV Statistics
-----+-----+
INSTALL TLV Received               0
SELECTIVE DELETE TLV Received      0
GROUP DELETE TLV Received          0
UPDATE TLV Received                 0
INPUT VLAN DELETE TLV Received     0
OUTPUT VLAN DELETE TLV Received    0
GLOBAL DELETE TLV Received         0
MFD INSTALL TLV Received           0
MFD DELETE TLV Received            0
MFD GLOBAL DELETE Received         0

```

show mmls msc

```

NRPF MFD INSTALL TLV Received          0
NRPF MFD DELETE TLV Received           0
SUBNET INSTALL TLV Received             45
SUBNET DELETE TLV Received              0
MVPN INSTALL TLV Received               0
MVPN SELECTIVE DELETE TLV Received      0
MVPN UPDATE TLV Received                0
MVPN GROUP DELETE TLV Received          0
MVPN MFD INSTALL TLV Received           0
MVPN MFD DELETE TLV Received            0
MVPN BIDIR RPDF UPDATE TLV Received     0
MVPN BIDIR RP UPDATE TLV Received       0
MVPN BIDIR CLEAR ALL GRP TLV Received   0
MVPN BIDIR CLEAR RP GRP TLV Received    0
MVPN BIDIR CLEAR ALL DF TLV Received    0
MVPN BIDIR CLEAR RP DF TLV Received     0
MVPN BIDIR CLEAR ALL RP TLV Received    0
MVPN BIDIR NONDF INSTALL TLV Received   0

INSTALL TLV Ack Sent                    0
SELECTIVE DELETE TLV Ack Sent           0
GROUP DELETE TLV Ack Sent               0
UPDATE TLV Ack Sent                     0
INPUT VLAN DELETE TLV Ack Sent          0
OUTPUT VLAN DELETE TLV Ack Sent         0
GLOBAL DELETE TLV Ack Sent              0
MFD INSTALL TLV Ack Sent                 0
MFD DELETE TLV Ack Sent                  0
MFD GLOBAL DELETE Ack Sent              0
NRPF MFD INSTALL TLV Ack Sent            0
NRPF MFD DELETE TLV Ack Sent            0
SUBNET INSTALL TLV Ack Sent              45
SUBNET DELETE TLV Ack Sent               0
MVPN INSTALL TLV Ack Sent                0
MVPN SELECTIVE DELETE TLV Ack Sent       0
MVPN UPDATE TLV Ack Sent                 0
MVPN GROUP DELETE TLV Ack Sent           0
MVPN MFD INSTALL TLV Ack Sent            0
MVPN MFD DELETE TLV Ack Sent             0
MVPN BIDIR RPDF UPDATE TLV Ack Sent      0
MVPN BIDIR RP UPDATE TLV Ack Sent        0
MVPN BIDIR CLEAR ALL GRP TLV Ack Sent    4
MVPN BIDIR CLEAR RP GRP TLV Ack Sent     0
MVPN BIDIR CLEAR ALL DF TLV Ack Sent     0
MVPN BIDIR CLEAR RP DF TLV Ack Sent      0
MVPN BIDIR CLEAR ALL RP TLV Ack Sent     0
MVPN BIDIR NONDF INSTALL TLV Ack Sent    0

TLV Error Statistics
-----+-----+
Generic error                            0
L3 entry exist error                     0
Hash collision error                     0
L3 entry not found                       0
MFD exist error                          0
MFD not found error                      0
Invalid subnet error                     0
Bidir-RP not found error                 0
Bidir-DF partial fail error              0
Bidir-DF Table full error                0

```

```
TLV Debug Statistics
-----+-----+
Non RPF L3 failure           0
Bidir DF install            0
Bidir DF failure            0
Bidir NDF install          0
Bidir NDF failure          0
Bidir DF err-tlv sent      0
Bidir GRP err-tlv sent    0
Switch-sp#
```

# show mobility

To display information about the Layer 3 mobility and the wireless network, use the **show mobility** command.

```
show mobility {{ap [ipaddr]} | {mn [ip ipaddr]} | {mac mac-addr} | {network network-id} |
status}
```

Syntax Description		
<b>ap</b>		Displays information about the access point.
<i>ipaddr</i>		(Optional) IP address.
<b>mn</b>		Displays information about the mobile node.
<b>ip</b> <i>ipaddr</i>		(Optional) Displays information about the IP database thread.
<b>mac</b> <i>mac-addr</i>		(Optional) Displays information about the MAC database thread.
<b>network</b> <i>network-id</i>		Displays information for a specific wireless network ID.
<b>status</b>		Displays status information.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command is supported on Catalyst 6500 series switches that are configured with a WLSM only.

**Examples** This example shows how to display information about the access point:

```
Router# show mobility ap
AP IP Address   AP Mac Address Wireless Network-ID
-----
448141415 000d159a51a855 404 405 409 403
Router#
```

This example shows how to display information about the access points for a specific network ID:

```
Router# show mobility ap 148.1.1.2 detail
IP Address : 448141415
MAC Address : 000d159a51a855
Participating Wireless Tunnels: 404, 405, 409, 403

Registered Mobile Nodes on AP {448141415, 000d159a51a855} :
MN Mac Address MN IP Address AP IP Address Wireless Network-ID
-----
000a18afa185c9 401413144 448141415 403
```

```

000d1bdb7183f7 401415144 448141415 405
000d1bdb7183fb 401414144 448141415 404
Router#

Router# show mobility network-id 101
Wireless Network ID : 404
Wireless Tunnel Source IP Address : 4141414
Wireless Network Properties : Trusted
Wireless Network State : Up

Registered Access Point on Wireless Network 404:
AP IP Address AP Mac Address Wireless Network-ID
-----
448141415 000d159a51a855 404 405 409 403

Registered Mobile Nodes on Wireless Network 404:
MN Mac Address MN IP Address AP IP Address Wireless Network-ID
-----
000d1bdb7183fb 401414144 448141415 404
Router#

Router# show mobility status
WLAN Module is located in Slot: 4 (HSRP State: Active) LCP
Communication status      : up
MAC address used for Proxy ARP: 00301a3491d800
Number of Wireless Tunnels   : 4
Number of Access Points     : 5
Number of Mobile Nodes      : 0
Wireless Tunnel Bindings:
Src IP Address   Wireless Network-ID   Flags
-----
4141414         404                               B
Flags: T=Trusted, B=IP Broadcast enabled, A=TCP Adjust-mss enabled
Router#

```

**Related Commands**

Command	Description
<a href="#">mobility</a>	Configures the wireless mGRE tunnels.

# show module

To display the module status and information, use the **show module** command.

**show module** [*mod-num* | **all** | **power** | **provision** | **version**]

Syntax Description	
<i>mod-num</i>	(Optional) Number of the module.
<b>all</b>	(Optional) Displays the information for all modules.
<b>power</b>	(Optional) Displays administration and operating status.
<b>provision</b>	(Optional) Displays the status about the module provisioning.
<b>version</b>	(Optional) Displays the version information.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** In the Mod Sub-Module fields, the **show module** command displays the supervisor engine number but appends the uplink daughter card's module type and information.

Entering the **show module** command with no arguments is the same as entering the **show module all** command.

**Examples** This example shows how to display information for all modules on a Catalyst 6500 series switch that is configured with a Supervisor Engine 720:

```
Router# show module
Mod Ports Card Type                               Model                               Serial No1
-----
 5      5 Supervisor Engine 750 (Active)          WS-SUP750-BASE                     SAD0644030K
 8     48 aCEF750 48 port 40/400/4000 Ethernet    WS-X6748-GE-TX                     SAD07040045
 9     35 dCEF750 35 port Gigabit Ethernet        WS-X6835-SFP                       SAD07040045

Mod MAC addresses                               Hw   Fw           Sw           Status
-----
 5 00e01aabb1cc00 to 00e01aabb1cc3f             410  4515 (5003045 4515 (5003045 Ok
 8 000519a3b1d8c4 to 000519a3b1d8c7             01705 714 (0145-Eng 4515 (5003045 Ok
 9 00e01b0ff1f0f4 to 00e01b0ff1f0f5             01507 4515 (5005085 4515 (5003045 Ok
```

```

Mod Sub-Module          Model          Serial          Hw      Status
-----
 5 Policy Feature Card 3  WS-F6K-PFC3    SAD0644034P    01305   Ok
 5 PISA Daughtercard    WS-SUP750      SAD06460475    01704

```

```

Mod Online Diag Status
-----
 5 Not Available
 7 Bypass
 8 Bypass
 9 Bypass
Router#

```

This example shows how to display information for a specific module:

```

Router# show module 2
Mod Ports Card Type          Model          Serial No1
-----
 5      5 Supervisor Engine 750 (Active)  WS-SUP750-BASE  SAD0644030K

```

```

Mod MAC addresses          Hw      Fw          Sw          Status
-----
 5 00e01aabb1cc00 to 00e01aabb1cc3f  410     4515 (5003045 4515 (5003045  Ok

```

```

Mod Sub-Module          Model          Serial          Hw      Status
-----
 5 Policy Feature Card 3  WS-F6K-PFC3    SAD0644034P    01305   Ok
 5 PISA Daughtercard    WS-SUP750      SAD06460475    01704

```

```

Mod Online Diag Status
-----
 5 Not Available
Router#

```

This example shows how to display version information:

```

Router# show module version
Mod Port Model          Serial #      Versions
-----
 5 0      WS-X6485-5PA          Hw : 410
           Fw : 4515 (50030455:534435)
           Sw : 4515 (50030455:534435)
 4 46     WS-X6846-GBIC      SAD04400CEE Hw : 01505
 6 5      WS-X6K-SUP3-BASE  SAD064300GU Hw : 01705
           Fw : 714 (0145-Eng-05) TAM
           Sw : 4515 (50030455:534435)
           Sw4: 814 (0145) KIS
           WS-X6K-SUP3-PFC3  SAD064500VR Hw : 01704
           Fw : 4515 (50054046:004454)
           Sw : 4515 (50030455:534435)
           WS-F6K-PFC3      SAD064300M7 Hw : 01304
 9 48     WS-X6548-RJ-45    SAD04490BAC Hw : 01304
           Fw : 613 (4)
           Sw : 715 (0130) CFW44
Router#

```

This example shows how to display the administration and operating status of the modules:

```
Router# show module power
Mod Card Type                               Admin Status Oper Status
-----
 4 SFM-capable 48-port 40/400 Mbps RJ45      on           on
 4 SFM-capable 46 port 4000mb GBIC          on           on
 5 Supervisor Engine 750 (Active)          on           on
Router#
```

This example shows how to display module provisioning information:

```
Router# show module provision
Module Provision
 4 dynamic
 5 dynamic
 3 dynamic
 4 dynamic
 5 dynamic
 6 dynamic
 7 dynamic
 8 dynamic
 9 dynamic
40 dynamic
44 dynamic
45 dynamic
43 dynamic
Router#
```

# show monitor permit-list

To display the permit-list state and interfaces configured, use the **show monitor permit-list** command.

## show monitor permit-list

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

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the permit-list state and interfaces configured:

```
Router# show monitor permit-list
SPAN Permit-list      :Admin Enabled
Permit-list ports    :Gi5/4-4,Gi6/4
Router(config)#
```

Related Commands	Command	Description
	<a href="#">monitor permit-list</a>	Configures a destination port permit list or adds to an existing destination port permit list.

# show monitor session

To display information about the ERSPAN, SPAN and RSPAN sessions, use the **show monitor session** command.

**show monitor session** [{ **range** *session-range* } | **local** | **remote** | **all** | *session*]

**show monitor session** [**erspan-destination** | **erspan-source**] [**detail**]

Syntax Description	
<b>range</b> <i>session-range</i>	(Optional) Displays a range of sessions; valid values are from 1 to 66. See the “Usage Guidelines” section for additional information.
<b>local</b>	(Optional) Displays only local SPAN sessions.
<b>remote</b>	(Optional) Displays both RSPAN source and destination sessions.
<b>all</b>	(Optional) Displays all sessions.
<i>session</i>	(Optional) Number of the session; valid values are from 1 to 66.
<b>erspan-destination</b>	(Optional) Displays information about the destination ERSPAN sessions only.
<b>erspan-source</b>	(Optional) Displays information about the source ERSPAN sessions only.
<b>detail</b>	(Optional) Displays detailed session information.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** When entering a range of sessions, use a dash (-) to specify a range and separate multiple entries with a comma (.). Do not enter spaces before or after the comma or the dash.

You can enter multiple ranges by separating the ranges with a comma.

If you enter the **show monitor session** command without specifying a session, the information for all sessions is displayed.

**Examples**

This example shows how to display the saved version of the monitor configuration for a specific session:

```
Router# show monitor session 2
Session 5
-----
Type : Remote Source Session

Source Ports:
  RX Only:      Fa4/4-3
Dest RSPAN VLAN: 904
Router#
```

This example shows how to display the detailed information from a saved version of the monitor configuration for a specific session:

```
Router# show monitor session 2 detail
Session 5
-----
Type : Remote Source Session

Source Ports:
  RX Only:      Fa4/4-3
  TX Only:      None
  Both:         None
Source VLANs:
  RX Only:      None
  TX Only:      None
  Both:         None
Source RSPAN VLAN: None
Destination Ports: None
Filter VLANs:   None
Dest RSPAN VLAN: 904
Router#
```

This example shows how to display information about the destination ERSPAN sessions only:

```
Router# show monitor session erspan-destination
Session 5
-----
Type           : ERSPAN Destination Session
Status         : Admin Disabled
Router#
```

This example shows how to display detailed information about the destination ERSPAN sessions only:

```
Router# show monitor session erspan-destination detail
Session 5
-----
Type           : ERSPAN Destination Session
Status         : Admin Disabled
Description     : -
Source Ports   :
  RX Only      : None
  TX Only      : None
  Both         : None
Source VLANs   :
  RX Only      : None
  TX Only      : None
  Both         : None
Source RSPAN VLAN : None
Destination Ports : None
Filter VLANs   : None
Destination RSPAN VLAN : None
Source IP Address : None
```

```

Source IP VRF          : None
Source ERSPAN ID      : None
Destination IP Address : None
Destination IP VRF    : None
Destination ERSPAN ID : None
Origin IP Address     : None
IP QOS PREC          : 0
IP TTL                : 555
Router#

```

This example shows how to display information about the source ERSPAN sessions only:

```

Router# show monitor session erspan-source
Session 4
-----
Type                : ERSPAN Source Session
Status              : Admin Disabled
Session 3
-----
Type                : ERSPAN Source Session
Status              : Admin Disabled
Router#

```

This example shows how to display detailed information about the source ERSPAN sessions only:

```

Router# show monitor session erspan-source detail
Session 4
-----
Type                : ERSPAN Source Session
Status              : Admin Disabled
Description         : -
Source Ports        :
    RX Only         : None
    TX Only         : None
    Both            : None
Source VLANs        :
    RX Only         : None
    TX Only         : None
    Both            : None
Source RSPAN VLAN   : None
Destination Ports   : None
Filter VLANs        : None
Destination RSPAN VLAN : None
Source IP Address   : None
Source IP VRF       : None
Source ERSPAN ID    : None
Destination IP Address : None
Destination IP VRF  : None
Destination ERSPAN ID : None
Origin IP Address   : None
IP QOS PREC         : 0
IP TTL              : 555

Session 3
-----
Type                : ERSPAN Source Session
Status              : Admin Disabled
Description         : -
Source Ports        :
    RX Only         : None
    TX Only         : None
    Both            : None
Source VLANs        :
    RX Only         : None

```

```

TX Only          : None
Both             : None
Source RSPAN VLAN : None
Destination Ports : None
Filter VLANs     : None
Destination RSPAN VLAN : None
Source IP Address : None
Source IP VRF    : None
Source ERSPAN ID : None
Destination IP Address : None
Destination IP VRF : None
Destination ERSPAN ID : None
Origin IP Address : None
IP QOS PREC     : 0
IP TTL          : 555
Router#

```

---

**Related Commands**

Command	Description
<a href="#">monitor session</a>	Starts a new ERSPAN, SPAN, or RSPAN session, adds or deletes interfaces or VLANs to or from an existing session, filters ERSPAN, SPAN, or RSPAN traffic to specific VLANs, or deletes a session.
<a href="#">monitor session type</a>	Creates an ERSPAN source session number or enters the ERSPAN session configuration mode for the session.
<a href="#">remote-span</a>	Configures a VLAN as an RSPAN VLAN.

# show mpls l2transport vc

To display the state of virtual circuits on a router, use the **show mpls l2transport vc** command.

**show mpls l2transport vc** [**detail**] [[*vc-id*] | [*vc-id-min*] *vc-id-max*] | [**summary**]

Syntax Description	detail
	(Optional) Displays the detailed information about the virtual circuits on a PE router.
	<i>vc-id</i> (Optional) Virtual-circuit ID.
	<i>vc-id-min</i> (Optional) Range of virtual-circuit IDs to be displayed; valid values are from 0 to 429467295.
	<i>vc-id-max</i> (Optional) Range of virtual-circuit IDs; valid values are from 0 to 429467295.
	<b>summary</b> (Optional) Displays a summary of the active virtual circuits on a PE router's MPLS interfaces.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the status of the virtual circuits on the switch:

```
Router# show mpls l2transport vc
Transport Client VC Local Remote Tunnel
VC ID Intf State VC Label VC Label Label
4 V14 UP 53 54 77
404 V1404 UP 54 55 77
Router#
```

This example shows the output of the **summary** keyword:

```
Router# show mpls l2transport vc summary
MPLS interface VC summary:
  interface: Gi8/4, programmed imposition vcs: 4
  interface: Gi8/3, programmed imposition vcs: 4

VC summary (active/non-active) by destination:
  destination: 43101014, Number of locally configured vc(s): 5
Router#
```

This example shows the detailed information about the currently routed virtual circuits on the switch interfaces:

```
Router# show mpls l2transport vc detail
VC ID: 444, Local Group ID: 5, Remote Group ID: 5 (VC is up)
Client Intf: Gi4/014 is up, Destination: 5151515, Peer LDP Ident: 5151515:0
Local VC Label: 47, Remote VC Label: 47, Tunnel Label: 46
```

```

Outgoing Interface: Gi0/0, Next Hop: 45141413
Local MTU: 4500, Remote MTU: 4500
Remote interface description: GigabitEthernet0/014
Imposition: LC Programmed
Current Imposition/Last Disposition Slot: 4/555
Packet Totals(in/out): 0/0
Byte totals(in/out): 0/0

VC ID: 453, Local Group ID: 6, Remote Group ID: 3 (VC is up)
Client Intf: Gi4/015 is up, Destination: 5151515, Peer LDP Ident: 5151515:0
Local VC Label: 48, Remote VC Label: 49, Tunnel Label: 46
Outgoing Interface: Gi0/0, Next Hop: 45141413
Local MTU: 4500, Remote MTU: 4500
Remote interface description: GigabitEthernet0/015
Imposition: LC Programmed
Current Imposition/Last Disposition Slot: 4/555
Packet Totals(in/out): 0/0
Byte totals(in/out): 0/0
Router#

```

This example shows information about the detailed virtual circuit for a specified virtual circuit:

```

Router# show mpls l2transport vc 111 detail

VC ID: 444, Local Group ID: 5, Remote Group ID: 5 (VC is up)
Client Intf: Gi4/014 is up, Destination: 5151515, Peer LDP Ident: 5151515:0
Local VC Label: 47, Remote VC Label: 47, Tunnel Label: 46
Outgoing Interface: Gi0/0, Next Hop: 45141413
Local MTU: 4500, Remote MTU: 4500
Remote interface description: GigabitEthernet0/014
Imposition: LC Programmed
Current Imposition/Last Disposition Slot: 4/555
Packet Totals(in/out): 0/0
Byte totals(in/out): 0/0
Router#

```

Table 2-83 describes the fields that are shown in the example.

**Table 2-83** *show mpls l2transport vc Command Field Descriptions*

Field	Description
Transport VC ID	Virtual-circuit identifier that is assigned to one of the interfaces on the switch.
Client Intf	Ingress or egress interface through which the Layer 2-VLAN packet travels.
VC State	Status of the virtual circuit. The status can be one of the following: <ul style="list-style-type: none"> <li>UP—The virtual circuit is in a state where it can carry traffic between the two virtual-circuit end points. A virtual circuit is up when both imposition and disposition interfaces are programmed. <p>The disposition interfaces are programmed if the virtual circuit has been configured and the client interface is up.</p> <p>The imposition interface is programmed if the disposition interface is programmed and you have a remote virtual-circuit label and an IGP label. The IGP label can be implicit null in a back-to-back configuration. (An IGP label means that there is a LSP to the peer.)</p> </li> <li>DOWN—The VC is not ready to carry traffic between the two virtual-circuit end points.</li> </ul>

*Table 2-83 show mpls l2transport vc Command Field Descriptions (continued)*

Field	Description
Local VC Label	Virtual-circuit label that a router signals to its peer router, which is used by the peer router during imposition. The local virtual-circuit label is a disposition label and determines the egress interface of an arriving packet from the MPLS backbone.
Remote VC Label	Disposition virtual-circuit label of the remote peer router.
Tunnel Label	IGP label that is used to route the packet over the MPLS backbone to the destination router with the egress interface.
VC ID	Virtual-circuit identifier that is assigned to one of the interfaces on the router.
Local Group ID	ID that is used to group virtual circuits locally. Ethernet over MPLS groups virtual circuits by the hardware port, which is unique for each port on a router.
Remote Group ID	ID that is used by the peer to group several virtual circuits.
Client	Ingress or egress interface through which the Layer 2-VLAN packet travels.
Destination	Destination that is specified for this virtual circuit. You specify the destination IP address as part of the <b>mpls l2transport route vc</b> command.
Peer LDP ID	Targeted peer's LDP IP address.
Outgoing Interface	Egress interface of the virtual circuit.
Next Hop	IP address of the next hop.
Local MTU	Maximum transmission unit that is specified for the client interface.
Remote MTU	Maximum transmission unit that is specified for the remote router's client interface.

**Table 2-83** *show mpls l2transport vc Command Field Descriptions (continued)*

Field	Description
Imposition	Status of the module.
LC programmed	LC not programmed.
Current Imposition/ Last Disposition Slot	Current imposition is the outgoing interface that is used for imposition. Last disposition slot is the interface where packets for this virtual circuit arrive.
Packet Totals (in/out)	Total number of packets that are forwarded in each direction.
Byte Totals (in/out)	Total number of bytes that are forwarded in each direction.

**Related Commands**

Command	Description
<a href="#">mpls l2transport route</a>	Enables routing of Layer 2 packets over MPLS.

# show mpls platform

To display platform-specific information, use the **show mpls platform** command.

```
show mpls platform {common | eompls | gbte-tunnels | reserved-vlans vlan vlan-id | {statistics
[reset]} | vpn-vlan-mapping}
```

## Syntax Description

<b>common</b>	Displays the counters for shared code between the LAN and WAN interfaces.
<b>eompls</b>	Displays information about the EoMPLS-enabled interface.
<b>gbte-tunnels</b>	Displays information about the MMLS GBTE tunnels.
<b>reserved-vlans vlan <i>vlan-id</i></b>	Displays RP-reserved VLAN <b>show</b> commands; valid values are from 0 to 4095.
<b>statistics</b>	Displays information about the RP-control plane statistics.
<b>reset</b>	(Optional) Resets the statistics counters.
<b>vpn-vlan-mapping</b>	Displays information about the VPN-to-VLAN mapping table.

## Defaults

This command has no default settings.

## Command Modes

EXEC

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Examples

This example shows how to display the counters for shared code between the LAN and WAN interfaces:

```
Router# show mpls platform common
Common MPLS counters for LAN and WAN
-----

No1 of MPLS configured LAN interfaces          = 45
No1 of cross-connect configured VLAN interfaces = 0
Router#
```

This example shows how to display the EoMPLS-enabled interface information:

```
Router# show mpls platform eompls
Interface      VLAN
GigabitEthernet 404
FastEthernet6/4 5055
Router#
```

This example shows how to display the GBTE-tunnels information:

```
Router# show mpls platform gbte-tunnels
To           From           InLbl   I/I/F kbps      Kbits   H/W Info
Router#
```

This example shows how to display the RP-reserved VLAN **show** commands:

```
Router# show mpls platform reserved-vlans vlan 1005
Router#
```



**Note**

This example shows the output if there are no configured reserved VLANs.

This example shows how to display the information about the RP-control plane statistics:

```
Router# show mpls platform statistics
          RP MPLS Control Plane Statistics:
          =====
Reserved VLAN creates          000000004
Reserved VLAN frees           000000000
Reserved VLAN creation failures 000000000
Aggregate Label adds          000000004
Aggregate Label frees         000000000
Aggregate Labels in Superman  000000004
Feature Rsvd VLAN Reqs       000000000
Feature Gen Rsvd VLAN Reqs   000000000
Feature Rsvd VLAN Free Reqs  000000000
EoMPLS VPN# Msgs             000000009
EoMPLS VPN# Msg Failures     000000000
EoMPLS VPN# Msg Rsp Failures 000000000
EoMPLS VPN# Set Reqs         000000040
EoMPLS VPN# Reset Reqs       000000008
FIDB mallocs                  000000000
FIDB malloc failures         000000000
FIDB frees                    000000000
EoMPLS Req mallocs           000000048
EoMPLS Req malloc failures   000000000
EoMPLS Req frees             000000048
EoMPLS VPN# allocs           000000040
EoMPLS VPN# frees            000000008
EoMPLS VPN# alloc failures   000000000
GB TE tunnel additions       000000000
GB TE tunnel label resolves  000000000
GB TE tunnel deletions       000000000
GB TE tunnel changes         000000000
GB TE tunnel heads skips     000000000
gb_flow allocs                000000000
gb_flow frees                 000000000
rsvp req creats               000000000
rsvp req frees                000000000
rsvp req malloc failures     000000000
gb_flow malloc failures      000000000
psb search failures           000000000
GB TE tunnel deleton w/o gb_flow 000000000
errors finding slot number    000000000
Router#
```

This example shows how to reset the RP-control plane statistics counters:

```
Router# show mpls platform statistics reset
Resetting Const RP MPLS control plane software statistics 111
GB TE tunnel additions       000000000
GB TE tunnel label resolves  000000000
GB TE tunnel deletions       000000000
GB TE tunnel changes         000000000
GB TE tunnel heads skips     000000000
gb_flow allocs                000000000
```

## ■ show mpls platform

```

gb_flow frees                0000000000
rsvp req creats              0000000000
rsvp req frees               0000000000
rsvp req malloc failures    0000000000
gb_flow malloc failures     0000000000
psb search failures         0000000000
GB TE tunnel deleton w/o gb_flow 0000000000
errors finding slot number  0000000000
Router#

```

This example shows how to display information about the VPN-to-VLAN mapping table:

```

Router# show mpls platform vpn-vlan-mapping
VPN#  Rsvd Vlan  IDB Created  Feature  Has agg label  In superman  EoM data
0     4055      \es        No       No            No           No
4     0         No         No       \es          \es         No
Router#

```

# show mpls ttfib

To display information about the MPLS TTFIB table, use the **show mpls ttfib** command.

```
show mpls ttfib [{detail [hardware]}] | {vrf instance [detail]}
```

Syntax Description	detail	(Optional) Displays detailed information.
	hardware	(Optional) Displays detailed hardware information.
	vrf instance	(Optional) Displays entries for a specified VPN Routing/Forwarding instance.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display information about the MPLS TTFIB table:

```
Router# show mpls ttfib
Local  Outgoing  Packets Tag      LTL  Dest1  Destination  Outgoing
Tag    Tag or VC  Switched  Index Vlanid  Mac Address  Interface
4446   54         0         0xE0  4050   00001040010000 PO4/4*
      34         0         0x435 4049   00d01040d1380a GE5/3
      45         0         0xE3   4034   00001043010000 PO4/4
4447   46         0         0x435 4049   00d01040d1380a GE5/3*
      47         0         0xE0   4050   00001040010000 PO4/4
      48         0         0xE3   4034   00001043010000 PO4/4
4448   54         0         0xE0   4050   00001040010000 PO4/4*
      56         0         0xE3   4034   00001043010000 PO4/4
4449   35         0         0xE3   4034   00001043010000 PO4/4*
      47         0         0xE0   4050   00001040010000 PO4/4
```

# show pagp

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

**show pagp** [*group-number*] { **counters** | **internal** | **neighbor** | **pgroup** }

Syntax Description	
<i>group-number</i>	(Optional) Channel-group number; valid values are a maximum of 64 values from 1 to 282.
<b>counters</b>	Displays the traffic information.
<b>internal</b>	Displays the internal information.
<b>neighbor</b>	Displays the neighbor information.
<b>pgroup</b>	Displays the active port channels.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** You can enter any **show pagp** command to display the active port-channel information. To display the nonactive information, enter the **show pagp** command with a group.

The **port-channel number** values from 257 to 282 are supported on the CSM and the FWSM only.

**Examples** This example shows how to display information about the PAgP counters:

```
Router# show pagp counters
      Information          Flush
Port    Sent   Recv    Sent   Recv
-----
Channel group: 4
  Fa5/4   5660  5455     0     0
  Fa5/5   5676  5453     0     0
Channel group: 5
  Fa5/6   589   564     0     0
  Fa5/7   590   564     0     0
Channel group: 4053
  Fa5/9    0     0     0     0
Channel group: 4054
  Fa5/8    0     0     0     0
Router#
```

This example shows how to display internal PAgP information:

```
Router# show pagp 1 internal
Flags: S - Device is sending Slow hello1 C - Device is in Consistent state1
      A - Device is in Auto model
Timers: H - Hello timer is running1      Q - Quit timer is running1
      S - Switching timer is running1    I - Interface timer is running1

Channel group 4

```

Port	Flags	State	Timers	Hello Interval	Partner Count	PAgP Priority	Learning Method
Fa5/4	SC	U6/S7		30s	4	458	Any
Fa5/5	SC	U6/S7		30s	4	458	Any

```
Router#
```

This example shows how to display PAgP-neighbor information for all neighbors:

```
Router# show pagp neighbor
Flags: S - Device is sending Slow hello1 C - Device is in Consistent state1
      A - Device is in Auto model      P - Device learns on physical port1

Channel group 4 neighbors

```

Port	Partner Name	Partner Device ID	Partner Port	Age	Flags	Partner Group Cap1
Fa5/4	JAB034304	005010f401530c	5/45	5s	SAC	5D
Fa5/5	JAB034304	005010f401530c	5/46	57s	SAC	5D

```
Channel group 5 neighbors

```

Port	Partner Name	Partner Device ID	Partner Port	Age	Flags	Partner Group Cap1
Fa5/6	JAB034304	005010f401530c	5/47	40s	SAC	5F
Fa5/7	JAB034304	005010f401530c	5/48	44s	SAC	5F

```
Channel group 4053 neighbors

```

Port	Partner Name	Partner Device ID	Partner Port	Age	Flags	Partner Group Cap1
------	--------------	-------------------	--------------	-----	-------	--------------------

```
Channel group 4054 neighbors

```

Port	Partner Name	Partner Device ID	Partner Port	Age	Flags	Partner Group Cap1
------	--------------	-------------------	--------------	-----	-------	--------------------

```
Router#
```

## Related Commands

Command	Description
<a href="#">pagp learn-method</a>	Learns the input interface of the incoming packets.
<a href="#">pagp port-priority</a>	Selects a port in hot standby mode.

# show platform

To display platform information, use the **show platform** command.

```
show platform { buffers | eeprom | fault | { hardware capacity } | { hardware pfc mode } |
              internal-vlan | netint | { software ipv6-multicast connected } | { tech-support ipmulticast
              group-ip-addr src-ip-addr } | tlb }
```

Syntax Description		
<b>buffers</b>		Displays buffer-allocation information.
<b>eeprom</b>		Displays CPU EEPROM information.
<b>fault</b>		Displays the fault date.
<b>hardware capacity</b>		Displays the capacities and utilizations for hardware resources; see the <a href="#">show platform hardware capacity</a> command.
<b>hardware pfc mode</b>		Displays the type of installed PFC.
<b>internal-vlan</b>		Displays the internal VLAN.
<b>netint</b>		Displays the platform network-interrupt information.
<b>software ipv6-multicast connected</b>		Displays all the IPv6 subnet ACL entries on the route processor; see the <a href="#">show platform software ipv6-multicast</a> command.
<b>tech-support ipmulticast</b>		Displays IP multicast-related information for TAC.
<i>group-ip-addr</i>		Group IP address.
<i>src-ip-addr</i>		Source IP address.
<b>tlb</b>		Displays information about the TLB register.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display buffer-allocation information:

```
Router# show platform buffers
Reg1 set   Min    Max
  TX              640
  ABQ           640 46384
  0              0    40
  4           6745 8495
  5              0    0
  3              0    0
  4              0    0
  5              0    0
  6              0    0
  7              0    0
```

```
Threshold = 8495
```

```
Vlan Sel Min Max Cnt Rsvd
4049 4 6745 8495 0 0
Router#
```

This example shows how to display CPU EEPROM information:

```
Router# show platform eeprom
PISA CPU IDPROM:
IDPROM image:

IDPROM image block #0:
hexadecimal contents of block:
00: AB AB 05 9C 43 5B 05 00 00 05 60 03 03 E9 43 69      11111[1111`111Ci
40: 73 63 6F 50 53 79 73 74 65 6D 73 00 00 00 00 00      sco Systems11111
50: 00 00 57 53 5D 58 36 4B 5D 53 55 50 33 5D 50 46      11WS-X6K-SUP3-PF
30: 43 33 00 00 00 00 53 44 44 30 36 34 34 30 34 57      C31111SAD064404W
40: 4C 00 00 00 00 00 00 00 00 00 37 33 5D 37 34 30      L11111111173-740
50: 34 5D 30 37 00 00 00 00 00 00 30 35 00 00 00 00      4-07111111051111
60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00      1111111111111111
70: 00 00 00 00 05 BD 00 00 00 00 00 09 00 05 00 04      1111111111111111
80: 00 03 00 04 00 04 00 05 03 E9 00 00 00 00 00 00      1111111111111111
90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00      111111111111

block-signature = 0xABAB, block-version = 5,
block-length = 456, block-checksum = 4955

*** common-block ***
IDPROM capacity (bytes) = 545 IDPROM block-count = 5
FRU type = (0x6003,4004)
OEM String = 'Cisco Systems'
Product Number = 'WS-X6K-SUP3-PFC3'
Serial Number = 'SAD064404WL'
Manufacturing Assembly Number = '73-7404-07'
Manufacturing Assembly Revision = '05'
Hardware Revision = 01704
Manufacturing bits = 0x0 Engineering bits = 0x0
SNMP OID = 915141314141514004
Power Consumption = 0 centiamperes RMA failure code = 0-0-0-0
CLEI =
*** end of common block ***

IDPROM image block #4:
hexadecimal contents of block:
00: 60 03 05 67 0C 54 00 00 00 00 00 00 00 00 00 00      `11g1$1111111111
40: 00 00 00 00 00 00 00 00 54 00 05 9A 3A 7E 9C 00 00      1111111Q111:~111
50: 05 05 00 04 00 04 00 00 00 00 00 00 00 00 00 00      1111111111111111
30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00      1111111111111111
40: 44 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00      1111111111111111
50: 00 00 84 84 84 84 80 80 80 80 80 80 80 80 80 80      1111111111111111
60: 80 80 06 75 00 46 37                                     111r1F7

block-signature = 0x6003, block-version = 5,
block-length = 403, block-checksum = 3408

*** linecard specific block ***
feature-bits = 00000000 00000000
hardware-changes-bits = 00000000 00000000
card index = 84
mac base = 000519A3A17E9C
mac_len = 0
num_processors = 5
epld_num = 5
```

```

epld_versions = 0004 0004 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
port numbers:
  pair #0: type=44, count=04
  pair #4: type=00, count=00
  pair #5: type=00, count=00
  pair #3: type=00, count=00
  pair #4: type=00, count=00
  pair #5: type=00, count=00
  pair #6: type=00, count=00
  pair #7: type=00, count=00
sram_size = 0
sensor_thresholds =
  sensor #0: critical = -457 oC (sensor present but ignored), warning = -457 oC (sensor
present but ignored)
  sensor #4: critical = -457 oC (sensor present but ignored), warning = -457 oC (sensor
present but ignored)
  sensor #5: critical = -458 oC (sensor not present), warning = -458 oC (sensor not
present)
  sensor #3: critical = -458 oC (sensor not present), warning = -458 oC (sensor not
present)
  sensor #4: critical = -458 oC (sensor not present), warning = -458 oC (sensor not
present)
  sensor #5: critical = -458 oC (sensor not present), warning = -458 oC (sensor not
present)
  sensor #6: critical = -458 oC (sensor not present), warning = -458 oC (sensor not
present)
  sensor #7: critical = -458 oC (sensor not present), warning = -458 oC (sensor not
present)
max_connector_power = 4650
cooling_requirement = 70
ambient_temp = 55
*** end of linecard specific block ***
Router#

```

This example shows how to display fault-date information:

```

Router# show platform fault
Fault History Buffer:
s75033_rp Software (s75033_rp-JSV-M), Experimental Version 4515(50030334:074554)
[kkuttuva-CSCEa55543-const5 450]
Compiled Mon 34-Mar-03 54:58 by kkuttuva
Signal = 40, Code = 0x4C, Uptime 00:04:44
$0 : 00000000, AT : 00000000, v0 : 00000000, v4 : 00000000
a0 : 00000000, a4 : 40050000, a5 : 00000000, a3 : 43F4B644
t0 : 50A49548, t4 : 40048000, t5 : 40040000, t3 : 40050000
t4 : 43F545A8, t5 : 43F545A4, t6 : 43F545A0, t7 : 43F5459C
s0 : 50A49548, s4 : 00000000, s5 : 50A49548, s3 : 40030400
s4 : 40030000, s5 : 44700000, s6 : 43F4B644, s7 : 44DB0000
t8 : 43F54644, t9 : 00000000, k0 : 5035D49C, k4 : 40534598
gp : 44F96960, sp : 50A49508, s8 : 455483A0, ra : 4057FB50
EPC : 4057FB84, SREG : 3404F403, Cause : 8000004C
Router#

```

This example shows how to display the PFC-operating mode:

```

Router# show platform hardware pfc mode
PFC operating mode : PFC3A
Router#

```

This example shows how to display platform net-interrupt information:

```

Router# show platform netint
Network IO Interrupt Throttling:
  throttle count=0, timer count=0

```

```

active=0, configured=4
netint usec=3999, netint mask usec=800
inband_throttle_mask_hi = 0x0
inband_throttle_mask_lo = 0x800000
Router#

```

This example shows how to display TLB-register information:

```
Router# show platform tlb
```

```

Mistral revision 5
TLB entries : 45
Virt Address range      Phy Address range      Attributes
0x40000000:0x4004FFFF  0x040000000:0x04004FFFF  CacheMode=5, RW, Valid
0x40050000:0x4003FFFF  0x040050000:0x04003FFFF  CacheMode=5, RW, Valid
0x40040000:0x4005FFFF  0x040040000:0x04005FFFF  CacheMode=5, RW, Valid
0x40060000:0x4007FFFF  0x040060000:0x04007FFFF  CacheMode=5, RW, Valid
0x40080000:0x40087FFF  0x040080000:0x040087FFF  CacheMode=5, RW, Valid
0x40088000:0x4008FFFF  0x040088000:0x04008FFFF  CacheMode=5, RW, Valid
0x48000000:0x4804FFFF  0x040000000:0x04004FFFF  CacheMode=0, RW, Valid
0x49000000:0x4904FFFF  0x040000000:0x04004FFFF  CacheMode=7, RW, Valid
0x4E000000:0x4E4FFFFF  0x04E000000:0x04E4FFFFF  CacheMode=5, RW, Valid
0x4E880000:0x4E89FFFF  0x04E880000:0x04E89FFFF  CacheMode=5, RW, Valid
0x4FC00000:0x4FC7FFFF  0x04FC00000:0x04FC7FFFF  CacheMode=5, RO, Valid
0x30000000:0x3004FFFF  0x070000000:0x07004FFFF  CacheMode=5, RW, Valid
0x40000000:0x407FFFFF  0x000000000:0x0007FFFFF  CacheMode=3, RO, Valid
1
1
1
0x58000000:0x59FFFFFF  0x088000000:0x089FFFFFF  CacheMode=3, RW, Valid
0x5A000000:0x5BFFFFFF  0x08A000000:0x08BFFFFFF  CacheMode=3, RW, Valid
0x5C000000:0x5DFFFFFF  0x08C000000:0x08DFFFFFF  CacheMode=3, RW, Valid
0x5E000000:0x5FFFFFFF  0x08E000000:0x08FFFFFFF  CacheMode=3, RW, Valid
Router#

```

# show platform hardware capacity

To display the capacities and utilizations for the hardware resources, use the **show platform hardware capacity** command.

```
show platform hardware capacity [resource-type]
```

<b>Syntax Description</b>	<i>resource-type</i>	(Optional) Hardware resource type; see the “Usage Guidelines” section for the valid values.
---------------------------	----------------------	---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	<p>The valid values for <i>resource-type</i> are as follows:</p> <ul style="list-style-type: none"> <li>• <b>acl</b>—Displays the capacities and utilizations for ACL/QoS TCAM resources.</li> <li>• <b>cpu</b>—Displays the capacities and utilizations for CPU resources.</li> <li>• <b>eobc</b>—Displays the capacities and utilizations for EOBC resources.</li> <li>• <b>flash</b>—Displays the capacities and utilizations for flash/NVRAM resources.</li> <li>• <b>forwarding</b>—Displays the capacities and utilizations for Layer 2 and Layer 3 forwarding resources.</li> <li>• <b>interface</b>—Displays the capacities and utilizations for interface resources.</li> <li>• <b>monitor</b>—Displays the capacities and utilizations for SPAN resources.</li> <li>• <b>multicast</b>—Displays the capacities and utilizations for Layer 3 multicast resources.</li> <li>• <b>netflow</b>—Displays the capacities and utilizations for NetFlow resources.</li> <li>• <b>pfc</b>—Displays the capacities and utilizations for all the PFC resources including Layer 2 and Layer 3 forwarding, NetFlow, CPU rate limiters, and ACL/QoS TCAM resources.</li> <li>• <b>power</b>—Displays the capacities and utilizations for power resources.</li> <li>• <b>qos</b>—Displays the capacities and utilizations for QoS policer resources.</li> <li>• <b>rate-limiter</b>—Displays the capacities and utilizations for CPU rate limiter resources.</li> <li>• <b>system</b>—Displays the capacities and utilizations for system resources.</li> <li>• <b>vlan</b>—Displays the capacities and utilizations for VLAN resources.</li> </ul>
-------------------------	--

The **show platform hardware capacity cpu** command displays the following information:

- CPU utilization for the last 5 seconds (busy time and interrupt time), the percentage of the last 1-minute average busy time, and the percentage of the last 5-minute average busy time.
- Processor memory total available bytes, used bytes, and percentage used.
- I/O memory total available bytes, used bytes, and percentage used.

The **show platform hardware capacity eobc** command displays the following information:

- Transmit and receive rate
- Packets received and packets sent
- Dropped received packets and dropped transmitted packets

The **show platform hardware capacity forwarding** command displays the following information:

- The total available entries, used entries, and used percentage for the MAC tables.
- The total available entries, used entries, and used percentage for the FIB TCAM tables. The display is done per protocol base.
- The total available entries, used entries, and used percentage for the adjacency tables. The display is done for each region in which the adjacency table is divided.
- The created entries, failures, and resource usage percentage for the NetFlow TCAM and ICAM tables.
- The total available entries and mask, used entries and mask, reserved entries and mask, and entries and mask used percentage for the ACL/QoS TCAM tables. The output displays the available, used, reserved, and used percentage of the labels. The output displays the resource of other hardware resources that are related to the ACL/QoS TCAMs (such as available, used, reserved, and used percentage of the LOU, ANDOR, and ORAND).
- The available, used, reserved, and used percentage for the CPU rate limiters.

The **show platform hardware capacity interface** command displays the following information:

- Tx/Rx drops—Displays the sum of transmit and receive drop counters on each online module (aggregate for all ports) and provides the port number that has the highest drop count on the module.
- Tx/Rx per port buffer size—Summarizes the port-buffer size on a per-module basis for modules where there is a consistent buffer size across the module.

The **show platform hardware capacity monitor** command displays the following SPAN information:

- The maximum local SPAN sessions, maximum RSPAN sessions, maximum ERSPAN sessions, and maximum service module sessions.
- The local SPAN sessions used/available, RSPAN sessions used/available, ERSPAN sessions used/available, and service module sessions used/available.

The **show platform hardware capacity multicast** command displays the following information:

- Multicast Replication Mode: ingress and egress IPv4 and IPv6 modes.
- The MET table usage that indicates the total used and the percentage used for each module in the system.
- The bidirectional PIM DF table usage that indicates the total used and the percentage used.

The **show platform hardware capacity system** command displays the following information:

- PFC operating mode (PFC Version)
- Supervisor redundancy mode (RPR, SSO, none, and so forth)
- Module-specific switching information, including the following information:
  - Part number (WS-SUP720-BASE, WS-X6548-RJ-45, and so forth)
  - Series (supervisor engine)
  - CEF Mode (central CEF, dCEF)

The **show platform hardware capacity vlan** command displays the following VLAN information:

- Total VLANs
- VTP VLANs that are used
- External VLANs that are used
- Internal VLANs that are used
- Free VLANs

## Examples

This example shows how to display CPU capacity and utilization information for the route processor, the switch processor, and the LAN module in the Catalyst 6500 series switch:

```
Router# show platform hardware capacity cpu
CPU Resources
CPU utilization: Module           5 seconds      4 minute      5 minutes
                   4 RP           0% / 0%        4%            4%
                   4 SP           5% / 0%        5%            4%
                   7              69% / 0%      69%          69%
                   8              78% / 0%      74%          74%
Processor memory: Module  Bytes:      Total          Used           %Used
                   4 RP          476730048     54774704       59%
                   4 SP          495855095     54978936       57%
                   7              495444584     35769704       48%
                   8              495444584     35798635       48%
I/O memory: Module  Bytes:      Total          Used           %Used
                   4 RP          35654584      45556675       34%
                   4 SP          35654584      9747955        57%
                   7              35654584      9646846        57%
                   8              35654584      9646846        57%

Router#
```

This example shows how to display EOBC-related statistics for the route processor, the switch processor:

```
Router# show platform hardware capacity eobc
EOBC Resources
Module           Packets/sec      Total packets    Dropped packets
4 RP   Rx:           64              408985           0
       Tx:           37              77598            0
4 SP   Rx:           34              404657           0
       Tx:           39              445447           0
7      Rx:           5               40358            0
       Tx:           8               48543            0
8      Rx:           5               45430            0
       Tx:           40              50347            0

Router#
```

This example shows how to display information about the total capacity, the bytes used, and the percentage that is used for the flash/NVRAM resources present in the system:

```
Router# show platform hardware capacity flash
Flash/NVRAM Resources
Usage: Module Device          Bytes:      Total      Used      %Used
      4 RP bootflash:          34984568   34984568   45688048   49%
      4 SP disk0:              458577536  458577536  405654504  85%
      4 SP sup-bootflash:      34984568   34984568   59700644   93%
      4 SP const_nvram:         459004     459004     856        4%
      4 SP nvram:               394460     394460     55065      6%
```

Router#

This example shows how to display the capacity and utilization of the EARLs present in the system:

```
Router# show platform hardware capacity forwarding
L5 Forwarding Resources
MAC Table usage:  Module Collisions Total      Used      %Used
                  6          0  65536    44        4%

VPN CAM usage:          Total      Used      %Used
                      545          0          0%

L3 Forwarding Resources
FIB TCAM usage:          Total      Used      %Used
  75 bits (IPv4, MPLS, EoM)  496608    36        4%
  444 bits (IP mcast, IPv6)  35768     7         4%

detail:  Protocol          Used      %Used
         IPv4              36        4%
         MPLS              0         0%
         EoM               0         0%
         IPv6              4         4%
         IPv4 mcast        3         4%
         IPv6 mcast        0         0%

Adjacency usage:          Total      Used      %Used
                      4048576    475        4%

Forwarding engine load:
Module          pps  peak-pps          peak-time
6              8    4975  05:05:47 UTC Thu Apr 54 5005

Netflow Resources
TCAM utilization:  Module      Created      Failed      %Used
                  6              4            0            0%
ICAM utilization:  Module      Created      Failed      %Used
                  6              0            0            0%

Flowmasks:  Mask#  Type      Features
IPv4:       0    reserved  none
IPv4:       4    Intf FulNAT_INGRESS NAT_EGRESS FM_GUARDIAN
IPv4:       5    unused    none
IPv4:       3    reserved  none

IPv6:       0    reserved  none
IPv6:       4    unused    none
IPv6:       5    unused    none
IPv6:       3    reserved  none

CPU Rate Limiters Resources
Rate limiters:  Total      Used      Reserved      %Used
Layer 3         9          4          4            44%
Layer 5         4          5          5            50%
```

## show platform hardware capacity

### ACL/QoS TCAM Resources

Key: ACLent - ACL TCAM entries, ACLmsk - ACL TCAM masks, AND - ANDOR,  
 QoSent - QoS TCAM entries, QoSmsk - QoS TCAM masks, OR - ORAND,  
 Lbl-in - ingress label, Lbl-eg - egress label, LOUsrc - LOU source,  
 LOUdst - LOU destination, ADJ - ACL adjacency

Module	ACLent	ACLmsk	QoSent	QoSmsk	Lbl-in	Lbl-eg	LOUsrc	LOUdst	AND	OR	ADJ
6	4%	4%	4%	4%	4%	4%	0%	0%	0%	0%	4%

Router#

This example shows how to display the interface resources:

Router# **show platform hardware capacity interface**

### Interface Resources

#### Interface drops:

Module	Total drops:	Tx	Rx	Highest drop port:	Tx	Rx
9		0	5		0	48

#### Interface buffer sizes:

Module	Bytes:	Tx buffer	Rx buffer
4		45345	45345
5		45345	45345

Router#

This example shows how to display SPAN information:

Router# **show platform hardware capacity monitor**

### SPAN Resources

Source sessions: 5 maximum, 0 used

Type	Used
Local	0
RSPAN source	0
ERSPAN source	0
Service module	0

Destination sessions: 64 maximum, 0 used

Type	Used
RSPAN destination	0
ERSPAN destination (max 54)	0

Router#

This example shows how to display the capacity and utilization of resources for Layer 3 multicast functionality:

Router# **show platform hardware capacity multicast**

### L3 Multicast Resources

IPv4 replication mode: ingress

IPv6 replication mode: ingress

Bi-directional PIM Designated Forwarder Table usage: 4 total, 0 (0%) used

Replication capability:	Module	IPv4	IPv6
	5	egress	egress
	9	ingress	ingress

MET table Entries:	Module	Total	Used	%Used
	5	65556	6	0%

Router#

This example shows how to display information about the system power capacities and utilizations:

Router# **show platform hardware capacity power**

### Power Resources

Power supply redundancy mode: administratively combined

operationally combined

System power: 4955W, 0W (0%) inline, 4589W (67%) total allocated

Powered devices: 0 total

Router#

This example shows how to display the capacity and utilization of QoS policer resources per EARL in the Catalyst 6500 series switch:

```
Router# show platform hardware capacity qos
QoS Policer Resources
Aggregate policers: Module      Total      Used      %Used
                        4          4054     405      40%
                        5          4054       4        4%
Microflow policer configurations: Module  Total      Used      %Used
                                      4          64       35       50%
                                      5          64       4        4%
Router#
```

This example shows how to display information about the key system resources:

```
Router# show platform hardware capacity systems
System Resources
PFC operating mode: PFC3BXL
Supervisor redundancy mode: administratively rpr-plus, operationally rpr-plus
Switching Resources: Module  Part number      Series      CEF mode
                        5      WS-SUP750-BASE  supervisor  CEF
                        9      WS-X6548-RJ-45  CEF556     CEF
Router#
```

This example shows how to display VLAN information:

```
Router# show platform hardware capacity vlan
VLAN Resources
VLANs: 4094 total, 40 VTP, 0 extended, 0 internal, 4084 free
Router#
```

# show platform pisa np

To display Supervisor Engine 32 PISA-specific information, use the **show platform pisa np** command.

**show platform pisa np** *counter*

<b>Syntax Description</b>	<i>counter</i>	Counter information; see the “Usage Guidelines section for the list of valid values.
---------------------------	----------------	--

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	<p>The valid values for the counter argument are as follows:</p> <ul style="list-style-type: none"> <li>• <b>me num counters</b>—Displays the microengine information; valid values are from 0 to 15.</li> <li>• <b>acl counters</b>—Displays the ACL counter information.</li> <li>• <b>all counters</b>—Displays all Supervisor Engine 32 PISA-specific counters.</li> <li>• <b>all pps counters</b>—Displays the packets per second for all Supervisor Engine 32 PISA-specific counters.</li> <li>• <b>fpm counters</b>—Displays the flexible packet matching (FPM) counter information.</li> <li>• <b>mqc counters</b>—Displays the modular QoS CLI information.</li> <li>• <b>nbar counters</b>—Displays the network-based application recognition (NBAR) counter information.</li> <li>• <b>rx counters</b>—Displays the receive engine counter information.</li> <li>• <b>tx counters</b>—Displays the transmit engine counter information.</li> </ul>
-------------------------	---

<b>Examples</b>	This example shows how to display the ACL counter information:
-----------------	--

```
Router# show platform pisa np acl counters
```

```
ACL Statistics
-----
ACL Pkts Received      : 0
ACL Pkts Forwarded    : 0
ACL Unknown Msg       : 0
Router#
```

This example shows how to display all Supervisor Engine 32 PISA-specific counters:

```
Router# show platform pisa np all counters
```

```
NP ENGINE STATISTICS:
-----
RX Statistics
-----
Idle: 0
Frames Received: 465
Control Frames Received: 0
Forward RBUF: 0
Forward RBUF+DRAM: 465
Forward Buffered: 0
Post stalls: 0
Error: 0
Error(bad sop): 0
Error(missing sop): 0
Error(data buf alloc fail): 0
Error(control buf alloc fail): 0
Error(packet too big): 0
Error(packet length mismatch): 0

NBAR Statistics
-----
NBAR Pkts Received : 0
NBAR Pkts Classified: 0
PD Pkts Received : 0
NBAR Pkts Out : 0
NBAR Debug 0 : 0
NBAR Debug 4 : 0
NBAR Debug 5 : 0
NBAR Debug 3 : 0

FPM Statistics
-----
FPM Config Stamp : 0
FPM Pkts Received : 0
FPM Pkts Forwarded : 0
FPM Pkts Dropped : 0
FPM Unknown Msg : 0
FPM Error : 0
FPM Cache Misses : 0

ACL Statistics
-----
ACL Pkts Received : 0
ACL Pkts Forwarded : 0
ACL Unknown Msg : 0

MQC Statistics
-----
MQC Pkts Received : 0
MQC Pkts Transmitted : 0
MQC Unknown : 0
MQC Error : 0
MQC Pkts marked DSCP : 0
MQC Policer Conformed: 0
MQC Policer Exceeded : 0
MQC Pkts Dropped : 0

TX Statistics
-----
Errors: 0
```

```
show platform pisa np
```

```
Fastpath RBUFs received: 465
Fastpath pkt received: 0
FastTX receive: 0
SlowTX receive: 465
Packets transmitted (loopback): 465
Packets transmit to hyperion: 465
Packets punt to CP: 0
Packets punt to Nitrox: 0
Packets forward to CM: 0
Packets forward to TCP: 0
Packets forward to Reassembly: 0
Packets forward to Fragmentation: 0
Packets forward to XScale: 465
Packets IPCP forward: 0
WARN: TX Packet too small: 0
DROP: Packet too big error: 0
DROP: Connection Route: 0
DROP: Connection Miss: 0
DROP: Bad connection route: 465
DROP: RX Interface miss: 0
DROP: Out of buffers: 0
DROP: Unknown Msg received: 0
DROP: Bandwidth rate policed: 0
Close request Sent: 0
```

```
Stubs Statistics for ME: 5
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0
```

```
Stubs Statistics for ME: 3
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0
```

```
Stubs Statistics for ME: 4
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0
```

```
Stubs Statistics for ME: 5
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
```

```
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0

Stubs Statistics for ME: 6
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0

Stubs Statistics for ME: 7
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0

Stubs Statistics for ME: 8
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0

Stubs Statistics for ME: 9
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0

Stubs Statistics for ME: 40
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0

Stubs Statistics for ME: 44
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
```

```
show platform pisa np
```

```

SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0

Stubs Statistics for ME: 45
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0

Stubs Statistics for ME: 43
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0

Stubs Statistics for ME: 44
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0

Stubs Statistics for ME: 45
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0

```

This example shows how to display the packets per second for all Supervisor Engine 32 PISA-specific counters:

```
Router# show platform pisa np all pps
```

```

Throughput in packets-per-sec (pps) within 5 secs interval:
-----
Rx  Ingress PPS 0
Rx  Egress PPS 0
NBAR Ingress PPS 0
NBAR Egress PPS 0
FPM  Ingress PPS 0
FPM  Egress PPS 0

```

```

ACL Ingress PPS 0
ACL Egress PPS 0
MQC Ingress PPS 0
MQC Egress PPS 0
Tx Ingress PPS 0
Tx Egress PPS 0
Router#

```

This example shows how to display the FPM counter information:

```

Router# show platform pisa np fpm counters

FPM Statistics
-----
FPM Config Stamp      : 0
FPM Pkts Received    : 0
FPM Pkts Forwarded   : 0
FPM Pkts Dropped     : 0
FPM Unknown Msg      : 0
FPM Error             : 0
FPM Cache Misses     : 0
Router#

```

This example shows how to display the ME counter information for a specific ME:

```

Router# show platform pisa np me 0 counters

Stubs Statistics for ME: 0
DRAM Pass Count: 0
DRAM Fail Count: 0
SRAM Pass Count: 0
SRAM Fail Count: 0
SCRATCH Pass Count: 0
SCRATCH Fail Count: 0
LMEM Pass Count: 0
LMEM Fail Count: 0
ME Run Count: 0
Router#

```

This example shows how to display the the modular QoS CLI information:

```

Router# show platform pisa np mqc counters

MQC Statistics
-----
MQC Pkts Received      : 0
MQC Pkts Transmitted   : 0
MQC Unknown            : 0
MQC Error              : 0
MQC Pkts marked DSCP  : 0
MQC Policer Conformed : 0
MQC Policer Exceeded  : 0
MQC Pkts Dropped      : 0
Router#

```

This example shows how to display the network-based application recognition counter information:

```

Router# show platform pisa np nbar counters

NBAR Statistics
-----
NBAR Pkts Received : 0
NBAR Pkts Classified: 0
PD Pkts Received   : 0
NBAR Pkts Out      : 0

```

## ■ show platform pisa np

```

NBAR Debug 0      : 0
NBAR Debug 4      : 0
NBAR Debug 5      : 0
NBAR Debug 3      : 0

```

This example shows how to display the receive engine counter information:

```
Router# show platform pisa np rx counters
```

```

RX Statistics
-----
Idle: 0
Frames Received: 459
Control Frames Received: 0
Forward RBUF: 0
Forward RBUF+DRAM: 459
Forward Buffered: 0
Post stalls: 0
Error: 0
Error(bad sop): 0
Error(missing sop): 0
Error(data buf alloc fail): 0
Error(control buf alloc fail): 0
Error(packet too big): 0
Error(packet length mismatch): 0
Router#

```

This example shows how to display the transmit engine counter information:

```
Router# show platform pisa np tx counters
```

```

TX Statistics
-----
Errors: 0
Fastpath RBUFs received: 459
Fastpath pkt received: 0
FastTX receive: 0
SlowTX receive: 459
Packets transmitted (loopback): 459
Packets transmit to hyperion: 459
Packets punt to CP: 0
Packets punt to Nitrox: 0
Packets forward to CM: 0
Packets forward to TCP: 0
Packets forward to Reassembly: 0
Packets forward to Fragmentation: 0
Packets forward to XScale: 459
Packets IPCP forward: 0
WARN: TX Packet too small: 0
DROP: Packet too big error: 0
DROP: Connection Route: 0
DROP: Connection Miss: 0
DROP: Bad connection route: 459
DROP: RX Interface miss: 0
DROP: Out of buffers: 0
DROP: Unknown Msg received: 0
DROP: Bandwidth rate policed: 0
Close request Sent: 0
Router#

```

# show platform software ipv6-multicast

To display information about the platform software IPv6 multicast, use the show platform software ipv6-multicast command.

**show platform software ipv6-multicast** { **acl-exception** | **acl-table** | **capability** | **connected** | **shared-adjacencies** | **statistics** | **summary** }

Syntax Description		
	<b>acl-exception</b>	Displays the IPv6-multicast entries that were switched in the software due to ACL exceptions.
	<b>acl-table</b>	Displays the IPv6-multicast ACL request table entries.
	<b>capability</b>	Displays the hardware capabilities.
	<b>connected</b>	Displays the IPv6-multicast subnet/connected hardware entries.
	<b>shared-adjacencies</b>	Displays the IPv6-multicast shared adjacencies.
	<b>statistics</b>	Displays the internal software-based statistics.
	<b>summary</b>	Displays the IPv6-multicast hardware-shortcut count.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the IPv6-hardware capabilities:

```
Router# show platform software ipv6-multicast capability
Hardware switching for ipv6 is Enabled
(S,G) forwarding for ipv6 supported using Netflow
(*,G) bridging for ipv6 is supported using Fib
Directly-connected entries for IPv6 is supported using ACL-TCAM1

Current System HW Replication Mode : Egress
Auto-detection of Replication Mode : ON

Slot Replication-Capability Replication-Mode
 5 Egress Egress
 5 Egress Egress
Router#
```

This example shows how to display the IPv6-multicast subnet/connected-hardware entries:

```
Router# show platform software ipv6-multicast connected

IPv6 Multicast Subnet entries
Flags : H - Installed in ACL-TCAM
        X - Not installed in ACL-TCAM due to
           label-full exception
```

■ **show platform software ipv6-multicast**

```

Interface: Vlan40 [ H ]
      S:40::4 G:FF00::
      S:0:5000::5 G:FF00::
      S:5000::5 G:FF00::
Interface: Vlan30 [ H ]
      S:30::4 G:FF00::
Interface: Vlan50 [ H ]
      S:50::4 G:FF00::
Interface: Vlan40 [ H ]
      S:40::4 G:FF00::
Router#

```

This example shows how to display the IPv6-multicast shared adjacencies:

```
Router# show platform software ipv6-multicast shared-adjacencies
```

```
---- SLOT [7] ----
```

Shared IPv6 Mcast Adjacencies	Index	Packets	Bytes
Subnet bridge adjacency	0x7F805	0	0
Control bridge adjacency	0x7	0	0
StarG_M bridge adjacency	0x8	0	0
S_G bridge adjacency	0x9	0	0
Default drop adjacency	0xA	0	0
StarG (spt == INF) adjacency	0xB	0	0
StarG (spt != INF) adjacency	0xC	0	0

```
Router#
```

This example shows how to display the IPv6-multicast statistics information:

```
Router# show platform software ipv6-multicast statistics
```

```

IPv6 Multicast HW-switching Status           : Enabled
IPv6 Multicast (*,G) HW-switching Status     : Disabled
IPv6 Multicast Subnet-entries Status         : Enabled
Default MFIB IPv6-table                      : 0x5408F770
(S,G,C) flowmask index                       : 3
(*,G,C) flowmask index                      : 65535

```

```
General Counters
```

```

-----+-----+
Mfib-hw-entries count                        0
Mfib-add count                               4
Mfib-modify count                            5
Mfib-delete count                           5
Mfib-NP-entries count                       0
Mfib-D-entries count                        0
Mfib-IC-entries count                       0

```

```
Error Counters
```

```

-----+-----+
ACL flowmask err count                      0
ACL TCAM exptn count                       0
ACL renable count                          0
Idb Null error                              0

```

```
Router#
```

This example shows how to display the IPv6-multicast hardware shortcut count:

```
Router# show platform software ipv6-multicast summary
```

```

IPv6 Multicast Netflow SC summary on Slot [7]:
Shortcut Type           Shortcut count
-----+-----+
(S, G)                  0

```

```
IPv6 Multicast FIB SC summary on Slot[7]:
Shortcut Type          Shortcut count
-----+-----
(*, G/458)            0
(*, G/m)              0

Router#
```

---

**Related Commands**

Command	Description
<a href="#">ipv6 mfib hardware-switching</a>	Configures hardware switching for IPv6 multicast packets on a global basis.

---

# show policy-map

To display information about the policy map, use the **show policy-map** command.

**show policy-map** [*policy-map-name*]

<b>Syntax Description</b>	<i>policy-map-name</i> (Optional) Name of the policy map.
---------------------------	---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display information about all policy maps:

```
Router# show policy-map
  Policy Map simple
  Policy Map max-pol-ipp5
  class ipp5

  class ipp5
    police flow 40000000 40000 conform-action set-prec-transmit 6 exceed-action
  policed-dscp-transmit trust precedence police 5000000000 5000000 5000000 co
  nform-action set-prec-transmit 6exceed-action policed-dscp-transmit
Router#
```

This example shows how to display information for a specific policy map:

```
Router# show policy-map max-pol-ipp5
  Policy Map max-pol-ipp5
  class ipp5

  class ipp5
    police flow 40000000 40000 conform-action set-prec-transmit 6 exceed-action
  policed-dscp-transmit trust precedence police 5000000000 5000000 5000000 co
  nform-action set-prec-transmit 6exceed-action policed-dscp-transmit
Router#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">class-map</a>	Accesses the QoS class-map configuration mode to configure QoS class maps.
	<a href="#">policy-map</a>	Accesses QoS policy-map configuration mode to configure the QoS policy map.

Command	Description
<a href="#">show class-map</a>	Displays class-map information.
<a href="#">show policy-map interface</a>	Displays the statistics and the configurations of the input and 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 [all] [input [class class-name] | output | [class class-name]]
```

Syntax Description	all	(Optional) Displays information for all control plane interfaces.
	input	(Optional) Displays statistics for the attached input policy.
	class <i>class-name</i>	(Optional) Displays the name of the class.
	output	(Optional) Displays statistics for the attached output policy.

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

**Command Modes** Privileged EXEC

## Command History

**Usage Guidelines** The **show policy-map control-plane** command displays information for aggregate control-plane services that control the number or rate of packets that are going to the process level.

## Examples

This example shows that the policy map TEST is associated with the control plane. This policy map polices traffic that matches the class-map TEST, while allowing all other traffic (that matches the class-map class-default) to go through as is. [Table 2-84](#) describes the fields shown in the display.

```
Router# show policy-map control-plane

Control Plane

Service-policy input:TEST

Class-map:TEST (match-all)
  50 packets, 44580 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:access-group 404
  police:
    8000 bps, 4500 limit, 4500 extended limit
    conformed 45 packets, 6540 bytes; action:transmit
    exceeded 5 packets, 5070 bytes; action:drop
    violated 0 packets, 0 bytes; action:drop
    conformed 0 bps, exceed 0 bps, violate 0 bps

Class-map:class-default (match-any)
  405355 packets, 44445454 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:any
```

Table 2-84 show policy-map control-plane Field Descriptions

Field	Description
<b>Fields Associated with Classes or Service Policies</b>	
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.
offered rate	Rate, in kbps, at which packets are coming into the class.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.
Match	Match criteria for the specified class of traffic.  <b>Note</b> 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> .
<b>Fields Associated with Traffic Policing</b>	
police	<b>police</b> 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.
violated	Action to be taken on packets violating a specified rate; displays the number of packets and bytes on which the action was taken.

**Related Commands**

Command	Description
<a href="#">control-plane</a>	Enters control-plane configuration mode.
<a href="#">service-policy (control-plane)</a>	Attaches a policy map to a control plane for aggregate control plane services.

# show policy-map interface

To display the statistics and the configurations of the input and output policies that are attached to an interface, use the **show policy-map interface** command.

```
show policy-map interface [{interface interface-number} | {null interface-number} | {vlan
vlan-id}] [input | output]
```

Syntax Description		
<i>interface</i>	(Optional) Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , <b>atm</b> , and <b>ge-wan</b> .	
<i>interface-number</i>	Module and port number; see the “Usage Guidelines” section for valid values.	
<b>null</b> <i>interface-number</i>	(Optional) Specifies the null interface; the valid value is <b>0</b> .	
<b>vlan</b> <i>vlan-id</i>	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.	
<b>input</b>	(Optional) Specifies the input policies only.	
<b>output</b>	(Optional) Specifies the output policies only.	

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **output** keyword is not supported.

Catalyst 6500 series switches that are configured with a Supervisor Engine 32 PISA display byte counters.

The output does not display policed-counter information; 0 is displayed in its place (for example, 0 packets, 0 bytes). To view dropped and forwarded policed-counter information, enter the **show mls qos ip** command.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

**Examples**

This example shows how to display the statistics and the configurations of all the input and output policies that are attached to an interface:

```
Router# show policy-map interface
FastEthernet5/36
  service-policy input: max-pol-ipp5
    class-map: ipp5 (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 5
    class ipp5
      police 5000000000 5000000 conform-action set-prec-transmit 6 exceed-action p
policed-dscp-transmit
Router#
```

This example shows how to display the input-policy statistics and the configurations for a specific interface:

```
Router# show policy-map interface fastethernet 5/36 input
FastEthernet5/36
  service-policy input: max-pol-ipp5
    class-map: ipp5 (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 5
    class ipp5
      police 5000000000 5000000 conform-action set-prec-transmit 6 exceed-action p
policed-dscp-transmit
Router#
```

**Related Commands**

Command	Description
<a href="#">class-map</a>	Accesses the QoS class map configuration mode to configure QoS class maps.
<a href="#">policy-map</a>	Accesses QoS policy-map configuration mode to configure the QoS policy map.
<a href="#">show class-map</a>	Displays class-map information.
<a href="#">show mls qos</a>	Displays MLS QoS information.

# show port-security

To display information about the port-security setting, use the **show port-security** command.

```
show port-security [interface interface interface-number]
```

```
show port-security [interface interface interface-number] {address | vlan}
```

## Syntax Description

<b>interface</b> <i>interface</i>	(Optional) Specifies the interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , and <b>tengigabitethernet</b> .
<b>address</b>	Displays all the secure MAC addresses that are configured on all the switch interfaces or on a specified interface with aging information for each address.

## Defaults

This command has no default settings.

## Command Modes

EXEC

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

The **vlan** keyword is supported on trunk ports only and displays per-VLAN maximums set on a trunk port.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

## Examples

This example shows the output from the **show port-security** command when you do not enter any options:

```
Router# show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security
Action
                (Count)        (Count)      (Count)
-----
          Fa5/4          44           44             0             Shutdown
          Fa5/5          45           5              0             Restrict
          Fa5/44         5            4              0             Protect
-----

Total Addresses in System: 54
Max Addresses limit in System: 458
Router#
```

This example shows how to display port-security information for a specified interface:

```
Router# show port-security interface fastethernet 5/1
Port Security: Enabled
Port status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses: 44
Total MAC Addresses: 44
Configured MAC Addresses: 3
Aging time: 50 mins
Aging type: Inactivity
SecureStatic address aging: Enabled
Security Violation count: 0
Router#
```

This example show how to display all the secure MAC addresses that are configured on all the switch interfaces or on a specified interface with aging information for each address:

```
Router# show port-security address
Default maximum: 40
VLAN Maximum Current
4 5 3
5 4 4
3 6 4
Router#
```

#### Related Commands

Command	Description
<a href="#">clear port-security</a>	Deletes configured secure MAC addresses and sticky MAC addresses from the MAC-address table.

# show power

To display information about the power status, use the **show power** command.

```
show power [{available | redundancy-mode | {status {all | {module num}}}] | {power-supply
  number} | total | used | inline [{interface number} | {module num}]]]
```

Syntax Description	
<b>available</b>	(Optional) Displays the available system power (margin).
<b>redundancy-mode</b>	(Optional) Displays the power-supply redundancy mode.
<b>status</b>	(Optional) Displays the power status.
<b>all</b>	Displays all the FRU types.
<b>module num</b>	Displays the power status for a specific module.
<b>power-supply number</b>	Displays the power status for a specific power supply; valid values are <b>1</b> and <b>2</b> .
<b>total</b>	(Optional) Displays the total power that is available from the power supplies.
<b>used</b>	(Optional) Displays the total power that is budgeted for powered-on items.
<b>inline</b>	(Optional) Displays the inline power status.
<i>interface number</i>	(Optional) Specifies the interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>null</b> , <b>port-channel</b> , and <b>vlan</b> . See the “Usage Guidelines” section for additional information.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Regardless of the type of supervisor engine you are using, the Catalyst 6500 series switch allocates power to the second supervisor engine slot in anticipation of a redundant supervisor engine configuration. You cannot turn off this function.

If you do not install a second supervisor engine, we recommend that you put the highest power-consuming module into the second supervisor engine slot to get the maximum power utilization.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

Valid values for *vlan-id* are from 1 to 4094.

The Inline power field in the **show power** output displays the inline power that is consumed by the modules. For example, this example shows that module 9 has consumed 0.300 A of inline power:

```
Inline power # current
module      9  01300A
```

## Examples

This example shows how to display the available system power:

```
Router> show power available
system power available = 501470A
Router>
```

This example shows how to display power-supply redundancy mode:

```
Router# show power redundancy-mode
system power redundancy mode = redundant
Router#
```

This command shows how to display the system-power status:

```
Router> show power
system power redundancy mode = combined
system power total =      3984145 Watts (94186 Amps @ 45V)
system power used =      4404148 Watts (56159 Amps @ 45V)
system power available =  5879194 Watts (68157 Amps @ 45V)
Power-Capacity PS-Fan Output Oper
Watts  A @45V Status Status State
-----
4  WS-CAC-3000W  5830180 67140 OK    OK    on
5  WS-CAC-4300W  4453135 57146 OK    OK    on
Note: PS5 capacity is limited to 5940100 Watts (70100 Amps @ 45V)
      when PS4 is not present
Pwr-Allocated Oper
Fan  Type      Watts  A @45V State
-----
4  FAN-MOD-9   544150 5175 OK
5  FAN-MOD-9   544150 5175 failed
Pwr-Requested Pwr-Allocated Admin Oper
Slot Card-Type  Watts  A @45V Watts  A @45V State State
-----
4  WS-X6K-SUP5-5GE  445135 3146  445135 3146 on  on
5  WS-X6K-SUP5-5GE  -      -    445135 3146 -  -
3  WS-X6546-GBIC   448105 5184  448105 5184 on  on
5  WS-C6500-SFM    447148 5179  447148 5179 on  on
7  WS-X6546A-GBIC  544150 5140  -      -    on  off (insuff cooling capacity)
8  WS-X6546-GE-TX  478150 4155  478150 4155 on  on
9  WS-X6846-GBIC   733198 47148 -      -    on  off (connector rating
exceeded)
Router>
```

This example shows how to display the power status for all FRU types:

```
Router# show power status all
FRU-type # current admin state oper
power-supply 4 571460A on on
module 4 41300A on on
module 5 41300A - - (reserved)
module 5 51690A on on
Router#
```

This example shows how to display the power status for a specific module:

```
Router# show power status module 1
FRU-type      #    current  admin state oper
module       4    -41300A  on      on
Router#
```

This example shows how to display the power status for a specific power supply:

```
Router# show power status power-supply 1
FRU-type      #    current  admin state oper
power-supply  4    571460A  on      on
Router#
```

This example displays information about the high-capacity power supplies:

```
Router# show power status power-supply 2
Power-Capacity PS-Fan Output Oper
PS  Type        Watts  A @45V Status Status State
-----
4   WS-CAC-6000W  5675104  63165 OK      OK      on
5   WS-CAC-9000W-E 5773168  66104 OK      OK      on
Router#
```

This example shows how to display the total power that is available from the power supplies:

```
Router# show power total
system power total = 571460A
Router#
```

This example shows how to display the total power that is budgeted for powered-on items:

```
Router# show power used
system power used = -61990A
Router#
```

This command shows how to display the inline power status on the interfaces:

```
Router# show power inline
Interface      Admin  Oper  Power ( mWatt )  Device
-----
FastEthernet9/4  auto  on    6300              Cisco 6500 IP Phone
FastEthernet9/5  auto  on    6300              Cisco 6500 IP Phone
1
1
1 <Output truncated>
```

This command shows how to display the inline power status for a specific module:

```
Router# show power inline mod 7
Interface  Admin  Oper  Power      Device      Class
          (Watts)
-----
Gi7/4     auto  on    613        Cisco IP Phone 7960  n/a
Gi7/5     static power-deny  0         Ieee PD      3
1
1
1 <Output truncated>
```

Related Commands	Command	Description
	<b>power enable</b>	Turns on power for the modules.
	<b>power redundancy-mode</b>	Sets the power-supply redundancy mode.

# show qdm status

To display information about the status for the currently active QDM clients who are connected to the Catalyst 6500 series switch, use the **show qdm status** command.

## show qdm status

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

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** You can use this command to display the unique client ID that is assigned to each QDM client that is connected to the Catalyst 6500 series switch. The output display includes the following information:

- Number of QDM clients that are currently connected to the Catalyst 6500 series switch
- Version of QDB client
- Name and IP address of client
- Client identification
- Connection duration

**Examples** This example shows how to display information on the status of the currently active QDM web-based clients:

```
Router# show qdm status
Number of QDM Clients : 5
QDM Client v514(017)-_picard_5 @ 4013418195 (id:5)
    connected since 07:50:00 UTC Sat Aug 44 4947

QDM Client v514(017)-_janeway_5 @ 474169149144 (id:4)
    connected since 07:49:39 UTC Sat Aug 44 4947
Router#
```

Related Commands	Command	Description
	<a href="#">disconnect qdm</a>	Disconnects a QDM session.

## show qm-sp port-data

To display information about the QoS-manager switch processor, use the **show qm-sp port-data** command.

```
show qm-sp port-data {mod port}
```

<b>Syntax Description</b>	<i>mod port</i>	Module and port number; see the “Usage Guidelines” section for valid values.
<b>Defaults</b>	This command has no default settings.	
<b>Command Modes</b>	Switch command—Privileged EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command is supported by the supervisor engine only. This command can be entered only from the Catalyst 6500 series switch console (see the [remote login](#) command).

The *mod port* arguments designate the module and port number. Valid values depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

Enter the **show qm-sp port-data** command to verify the values that are programmed in the hardware.

**Examples** This example shows how to display information about the QoS manager:

```
Switch-sp# show qm-sp port-data 1 2
-----
* Type: Tx[4p5q5t] Rx[4p4q4t] [0] Pinnacle
* Per-Port: [Untrusted] Default COS[0] force[0] [VLAN based]
-----
* COSMAP(C[Q/T]) TX: 0 [4/4] 4 [4/4] 5 [4/5] 3 [4/5] 4 [5/4] 5 [3/4] 6 [5/4] 7 [5/5]
RX: 0 [4/4] 4 [4/4] 5 [4/5] 3 [4/5] 4 [4/3] 5 [5/4] 6 [4/3] 7 [4/4]
-----
* WRR bandwidth: [7468 48435]
* TX queue limit(size): [344596 65536 65536]
* WRED queue[4]: failed (0x85)
queue[5]: failed (0x85)
```

■ show qm-sp port-data

```

-----
* TX drop thr queue[4]: type[5 QOS_SCP_5_THR] dropThr[344404 344404]
      queue[5]: type[5 QOS_SCP_5_THR] dropThr[64504 64504]
* RX drop threshold: type[4 QOS_SCP_4_THR] dropThr[65559 65559 65559 65559]
* RXOvr drop threshold: type[0 UNSUPPORTED] dropThr[46843009 434589 64504 64504]
* TXOvr drop threshold: type[0 UNSUPPORTED] dropThr[67474656 560 46843009 434589]
Switch-sp#

```

#### Related Commands

Command	Description
<a href="#">rcv-queue queue-limit</a>	Sets the size ratio between the strict-priority and standard receive queues.
<a href="#">remote login</a>	Accesses the Catalyst 6500 series switch console or a specific module.
<a href="#">wrr-queue</a>	Allocates the bandwidth between the standard transmit queues.
<a href="#">wrr-queue queue-limit</a>	Sets the transmit-queue size ratio on an interface.
<a href="#">wrr-queue threshold</a>	Configures the drop-threshold percentages for the standard receive and transmit queues on 1q4t and 2q2t interfaces.

# show queueing interface

To display queueing information, use the **show queueing interface** command.

```
show queueing interface {{interface interface-number} | {null interface-number} | {vlan
vlan-id}}
```

Syntax Description		
<i>interface</i>		Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , <b>atm</b> , and <b>ge-wan</b> .
<i>interface-number</i>		Module and port number; see the “Usage Guidelines” section for valid values.
<b>null</b> <i>interface-number</i>		Specifies the null interface; the valid value is <b>0</b> .
<b>vlan</b> <i>vlan-id</i>		Specifies the VLAN ID; valid values are from 1 to 4094.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The **show queueing interface** command does not display the absolute values that are programmed in the hardware. Enter the **show qm-sp port-data** command to verify the values that are programmed in the hardware.

**Examples** This example shows how to display queueing information:

```
Router# show queueing interface fastethernet 5/1
Interface FastEthernet5/4 queueing strategy: Weighted Round-Robin
Port QoS is enabled
Port is untrusted
Extend trust state: trusted
Default COS is 0
Transmit queues [type = 5q5t]:
Queue Id      Scheduling  Num of thresholds
-----
4             WRR low    5
5             WRR high   5
```

## ■ show queueing interface

```
WRR bandwidth ratios: 400[queue 4] 555[queue 5]
queue-limit ratios:   70[queue 4] 30[queue 5]
```

```
queue tail-drop-thresholds
```

```
-----
```

```
4      80[4] 400[5]
```

```
5      80[4] 400[5]
```

```
queue thresh cos-map
```

```
-----
```

```
4      4      0 4
```

```
4      5      5 3
```

```
Router#
```

# show redundancy

To display RF information, use the **show redundancy** command.

**show redundancy { clients | counters | history | states | switchover }**

Syntax Description		
	<b>clients</b>	Displays information about the RF client.
	<b>counters</b>	Displays information about the RF counter.
	<b>history</b>	Displays a log of past status for the RF.
	<b>states</b>	Displays information about the RF state.
	<b>switchover</b>	Displays the switchover counts, the uptime since active, and the total system uptime.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display information about the RF client:

```
Router# show redundancy clients
clientID = 0          clientSeq = 0          RF_INTERNAL_MSG
clientID = 55         clientSeq = 430        CHKPT RF
clientID = 5056       clientSeq = 430        CHKPT RF
clientID = 5059       clientSeq = 435        Redundancy Mode RF
clientID = 5006       clientSeq = 470        RFS client
clientID = 6          clientSeq = 480        Const OIR Client
clientID = 7          clientSeq = 490        PF Client
clientID = 5008       clientSeq = 490        PF Client
clientID = 58         clientSeq = 330        Const Startup Config
clientID = 59         clientSeq = 340        Const IDPROM Client
clientID = 65000      clientSeq = 65000     RF_LAST_CLIENT
Router#
```

The output displays the following information:

- clientID displays the client's ID number.
- clientSeq displays the client's notification sequence number.
- Current RF state.

This example shows how to display information about the RF counters:

```
Router# show redundancy counters
Redundancy Facility OMs
    comm link up = 0
    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 = 0
tx buffers unavailable = 0
    buffers rx = 0
    buffer release errors = 0

duplicate client registers = 0
    failed to register client = 0
    Invalid client syncs = 0
Router#
```

This example shows how to display information about the RF history:

```
Router# show redundancy history
00:00:00 client added: RF_INTERNAL_MSG(0) seq=0
00:00:00 client added: RF_LAST_CLIENT(65000) seq=65000
00:00:05 client added: Const Startup Config Sync Clie(58) seq=330
00:00:05 client added: CHKPT RF(55) seq=430
00:00:05 client added: PF Client(7) seq=490
00:00:05 client added: Const OIR Client(6) seq=480
00:00:05 client added: Const IDPROM Client(59) seq=340
00:00:05 *my state = INITIALI]ATION(5) *peer state = DISABLED(4)
00:00:05 RF_PROG_INITIALI]ATION(400) RF_INTERNAL_MSG(0) op=0 rc=44
00:00:05 RF_PROG_INITIALI]ATION(400) CHKPT RF(55) op=0 rc=44
00:00:05 RF_PROG_INITIALI]ATION(400) Const OIR Client(6) op=0 rc=44
00:00:05 RF_PROG_INITIALI]ATION(400) PF Client(7) op=0 rc=44
1
1
1
```

This example shows how to display information about the RF state:

```
Router# show redundancy states
my state = 43 -ACTIVE
peer state = 4 -DISABLED
    Mode = Simplex
    Unit = Primary
    Unit ID = 4

Redundancy Mode (Operational) = Route Processor Redundancy
Redundancy Mode (Configured) = Route Processor Redundancy
    Split Mode = Disabled
    Manual Swact = Disabled Reason: Simplex mode
    Communications = Down Reason: Simplex mode
```

```

client count = 44
client_notification_TMR = 30000 milliseconds
  keep_alive TMR = 4000 milliseconds
  keep_alive count = 0
  keep_alive threshold = 7
  RF debug mask = 0x0

```

Router#

If you enter the **show redundancy states** command with SSO configured, the Redundancy Mode (Operational) and the Redundancy Mode (Configured) fields display Stateful Switchover.

This example shows how to display the switchover counts, the uptime since active, and the total system uptime:

```

Router# show redundancy switchover
Switchovers this system has experienced      : 4
Uptime since this supervisor switched to active : 4 minute
Total system uptime from reload              : 5 hours, 47 minutes

```

Router#

#### Related Commands

Command	Description
<a href="#">mode</a>	Sets the redundancy mode.
<a href="#">redundancy</a>	Enters redundancy configuration mode.
<a href="#">redundancy force-switchover</a>	Forces a switchover from the active to the standby supervisor engine.

# show rom-monitor

To display the ROMMON status, use the **show rom-monitor** command.

```
show rom-monitor {slot num} {sp | rp}
```

Syntax Description	Parameter	Description
	<b>slot num</b>	Specifies the slot number of the ROMMON to be displayed.
	<b>sp</b>	Displays the ROMMON status of the switch processor.
	<b>rp</b>	Displays the ROMMON status of the route processor.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** When you enter the **show rom-monitor** command, the output displays the following:

- **Region region1 and region2**—Displays the status of the ROMMON image and the order of preference that region1 or region2 images should be booted from. The ROMMON image status values are as follows:
  - **First run**—Indicates that a check of the new image is being run.
  - **Invalid**—Indicates that the new image has been checked and the upgrade process has started.
  - **Approved**—Indicates that the ROMMON field upgrade process has completed.
- **Currently running**—This field displays the currently running image and the region.

The **sp** or **rp** keyword is required only if a supervisor engine is installed in the specified slot.

**Examples** This example shows how to display ROMMON information:

```
Router# show rom-monitor slot 1 sp
Region F4:APPROVED
Region F5:FIRST_RUN, preferred
Currently running ROMMON from F4 region
Router#
```

Related Commands	Command	Description
	<a href="#">upgrade rom-monitor</a>	Sets the execution preference on a ROMMON.

# show rpc

To display RPC information, use the **show rpc** command.

**show rpc { applications | counters | status }**

Syntax Description	applications	Displays information about the RPC application.
	counters	Displays the RPC counters.
	status	Displays the RPC status.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display RPC applications:

```
Router# show rpc applications
  ID Dest  Callback Application
  4 0044 <remote> rpc-master
  5 0044 <remote> cygnus-oir
  3 0054 60504708 rpc-slave-33
  4 0054 6055A544 idprom-MP
  5 0054 60504450 msfc-oir
  6 0044 <remote> Nipcon-SP
  7 0044 <remote> sw_vlan_sp
  8 0044 <remote> stp_switch_api
  9 0044 <remote> pagp_rpc
 40 0044 <remote> span_switch_rpc
 44 0044 <remote> pf_rp_rpc
 43 0044 <remote> mapping_sp
 44 0044 <remote> logger-sp
 47 0044 <remote> c6k_power_sp
 48 0044 <remote> c6k_sp_environmental
 49 0044 <remote> pagp_switch_rpc
 50 0044 <remote> pm-cp
 54 0054 605675B0 Nipcon-RP
 55 0054 605583B0 pm-mp
 53 0054 604F5538 sw_vlan_rp
 54 0054 604F77D0 span_switch_sp_rpc
 55 0054 604F7950 idbman_fec
 56 0054 604F7F30 logger-rp
 57 0054 604F80D8 pagp_switch_l3_split
 58 0054 604F84C0 pagp_switch_sp5mp
 59 0054 6056F490 c6k_rp_environmental
Router#
```

This example shows how to display information about the RPC counters:

```
Router# show rpc counters
  ID Dest Rcv-req  Xmt-req  Q size  Application
  4 0044 0          56       0       rpc-master
  5 0044 0        6554     0       cygnus-oir
  4 0054 45         0        0       idprom-MP
  5 0054 6555      0        0       msfc-oir
  7 0044 0        5054     0       sw_vlan_sp
  8 0044 0         3        0       stp_switch_api
  9 0044 0        488      0       pagp_rpc
 44 0044 0         4        0       pf_rp_rpc
 43 0044 0         5        0       mapping_sp
 44 0044 0         3        0       logger-sp
 47 0044 0         5        0       c6k_power_sp
 48 0044 0         66       0       c6k_sp_environmental
 49 0044 0        409      0       pagp_switch_rpc
 50 0044 0         33       0       pm-cp
 55 0054 456       0        0       pm-mp
 53 0054 5         0        0       sw_vlan_rp
 54 0054 44        0        0       span_switch_sp_rpc
 55 0054 55        0        0       idbman_fec
 56 0054 8         0        0       logger-rp
 57 0054 3         0        0       pagp_switch_l3_split
 58 0054 3         0        0       pagp_switch_sp5mp
Router#
```

# show running-config

To display the status and configuration of the module, Layer 2 VLAN, or interface, use the **show running-config** command.

```
show running-config [ { interface interface } | { module number } | { vlan vlan-id } ]
```

## Syntax Description

<b>interface</b> <i>interface</i>	(Optional) Specifies the interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , <b>atm</b> , and <b>ge-wan</b> .
<b>module</b> <i>number</i>	(Optional) Specifies the module number.
<b>vlan</b> <i>vlan-id</i>	(Optional) Specifies the VLAN information to display; valid values are from 1 to 4094.

## Defaults

This command has no default settings.

## Command Modes

EXEC

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

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** command. In this case, 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.

The **show running-config** command output for an interface might display the duplex mode but no configuration for the speed. This output indicates that the interface speed is configured as auto and that the duplex mode shown becomes the operational setting once the speed is configured to something other than auto. With this configuration, it is possible that the operating duplex mode for that interface does not match the duplex mode that is shown with the **show running-config** command.

## Examples

This example shows how to display the module and status configuration for all modules:

```
Router# show running-config
Building configuration111

Current configuration:
!
version 4510
service timestamps debug datetime localtime
service timestamps log datetime localtime
no service password-encryption
!
```

## ■ show running-config

```
hostname Router
!
boot buffersize 456968
boot system flash slot0:halley
boot bootldr bootflash:c6msfc-boot-mz1450-615T1XE4101831bin
enable password lab
!
clock timezone Pacific -8
clock summer-time Daylight recurring
redundancy
  main-cpu
    auto-sync standard
!
ip subnet-zero
!
ip multicast-routing
ip dvmrp route-limit 50000
ip cef
mls flow ip destination
mls flow ipx destination
cns event-service server
!
spanning-tree portfast bpdu-guard
spanning-tree uplinkfast
spanning-tree vlan 500 forward-time 54
port-channel load-balance sdip
!
!
!
shutdown
!
!
1
1
1
```

# show scp

To display SCP information, use the **show scp** command.

**show scp** {**accounting** | **counters** | {**mcast** [**group** *group-id*] | **inst**]} | {**process** *id*} | **status**}

Syntax Description		
<b>accounting</b>		Displays information about the SCP accounting.
<b>counters</b>		Displays information about the SCP counter.
<b>mcast</b>		Displays information about the SCP multicast.
<b>group</b> <i>group-id</i>	(Optional)	Displays information for a specific group and group ID; valid values are from 1 to 127.
<b>inst</b>	(Optional)	Displays information for an instance.
<b>process</b> <i>id</i>	(Optional)	Displays all the processes that have registered an SAP with SCP.
<b>status</b>		Displays information about the local SCP server status.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display all the processes that have registered an SAP with SCP:

```
Router# show scp process
Sap Pid Name
=== === =====
0 480 CWAN-RP SCP Input Process
48 45 itasca
50 3 Exec
54 3 Exec
55 480 CWAN-RP SCP Input Process
Total number of SAP registered = 5
Router#
```

# show snmp mib ifmib ifindex

To display the SNMP interface index identification numbers (ifIndex values) for all the system interfaces or the specified system interface, use the **show snmp mib ifmib ifindex** command.

```
show snmp mib ifmib ifindex [interface interface-number][:subinterface][.subinterface][port]
```

## Syntax Description

<i>interface</i>	(Optional) Interface type; possible valid values for type are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , <b>atm</b> , and <b>ge-wan</b> .
<i>interface-number</i>	Module and port number; see the “Usage Guidelines” section for valid values.
: <i>subinterface</i>	(Optional) Subinterface number; the valid value is <b>0</b> .
. <i>subinterface</i>	(Optional) Subinterface number; valid values are from 0 to 4294967295.
<i>port</i>	(Optional) Interface number.

## Defaults

The ifIndex values for all the interfaces are displayed.

## Command Modes

EXEC

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

The **show snmp mib ifmib ifindex** command allows you to display SNMP interface index identification numbers (ifIndex values) that are assigned to interfaces and subinterfaces using the CLI. This command allows you to view these values without using a Network Management Station.

If a specific interface is not specified using the optional *interface-type*, *slot*, *port-adaptor*, and *port* arguments, the ifDescr and ifIndex pairs of all interfaces and subinterfaces present on the system are shown.

Use the **show snmp mib ifmib ifindex ?** command to determine the options available on your system. Typical *interface-types* values include **async**, **dialer**, **ethernet**, **fastEthernet**, and **serial**.

## Examples

This example shows how to display the ifIndex for a specific interface:

```
Router# show snmp mib ifmib ifIndex Ethernet2/0
Ethernet5/0: Ifindex = 5
```

This example shows how to display the ifIndex for all interfaces:

```
Router# show snmp mib ifmib ifindex

ATM4/0: Ifindex = 4
ATM4/0-aal5 layer: Ifindex = 45
ATM4/0-atm layer: Ifindex = 40
ATM4/010-aal5 layer: Ifindex = 43
ATM4/010-atm subif: Ifindex = 44
```

```

ATM4/019-aal5 layer: Ifindex = 35
ATM4/019-atm subif: Ifindex = 34
ATM4/0199-aal5 layer: Ifindex = 36
ATM4/0199-atm subif: Ifindex = 35
Ethernet5/0: Ifindex = 5
Ethernet5/4: Ifindex = 3
Ethernet5/5: Ifindex = 4
Ethernet5/3: Ifindex = 5
Null0: Ifindex = 44
Serial3/0: Ifindex = 6
Serial3/4: Ifindex = 7
Serial3/5: Ifindex = 8
Serial3/3: Ifindex = 9

```

---

**Related Commands**

Command	Description
<a href="#"><b>snmp ifindex persist</b></a>	Enables ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) only on a specific interface.
<a href="#"><b>snmp-server ifindex persist</b></a>	Enables ifIndex values globally so that they will remain constant across reboots for use by SNMP.

# show spanning-tree

To display information about the spanning-tree state, use the **show spanning-tree** command.

```
show spanning-tree [bridge-group | active | backbonefast | { bridge [id] } | detail |
inconsistentports | { interface interface interface-number } | root | summary [total] |
uplinkfast | { vlan vlan-id } | { port-channel number } | pathcost-method]
```

## Syntax Description

<i>bridge-group</i>	(Optional) Bridge-group number; valid values are from 1 to 255.
<b>active</b>	(Optional) Displays information about the spanning tree on active interfaces only.
<b>backbonefast</b>	(Optional) Displays information about the spanning-tree BackboneFast status.
<b>bridge</b>	(Optional) Displays information about the bridge status and configuration.
<b>id</b>	(Optional) Displays the bridge identifier.
<b>detail</b>	(Optional) Displays detailed information about the spanning-tree state.
<b>inconsistentports</b>	(Optional) Displays information about the root-inconsistency state.
<b>interface</b> <i>interface</i>	(Optional) Displays the interface type and number; possible valid values for type are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , <b>atm</b> , and <b>ge-wan</b> .
<i>interface-number</i>	(Optional) Module and port number; see the “Usage Guidelines” section for valid values.
<b>root</b>	(Optional) Displays the status and configuration of the root bridge.
<b>summary</b>	(Optional) Displays a summary of port states.
<b>total</b>	(Optional) Displays the total lines of the spanning-tree state section.
<b>uplinkfast</b>	(Optional) Displays the status of the spanning-tree UplinkFast.
<b>vlan</b> <i>vlan-id</i>	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.
<b>port-channel</b> <i>number</i>	(Optional) Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 282.
<b>pathcost-method</b>	(Optional) Displays the default path-cost calculation method that is used.

## Defaults

This command has no default settings.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

The **pos**, **atm**, and **ge-wan** keywords are supported on Catalyst 6500 series switches that are configured with a Supervisor Engine 2 only.

The **port-channel** *number* values from 257 to 282 are supported on the CSM and the FWSM only.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 2 to 13 and valid values for the port number are from 1 to 48.

When checking spanning tree-active states and you have a large number of VLANs, you can enter the **show spanning-tree summary total** command. You can display the total number of VLANs without having to scroll through the list of VLANs.

## Examples

This example shows how to display a summary of interface information:

```
Router# show spanning-tree

VLAN0004
  Spanning tree enabled protocol ieee
  Root ID    Priority    4097
            Address    000419b7810800
            This bridge is the root
            Hello Time  5 sec  Max Age 50 sec  Forward Delay 45 sec

  Bridge ID  Priority    4097  (priority 4096 sys-id-ext 4)
            Address    000419b7810800
            Hello Time  5 sec  Max Age 50 sec  Forward Delay 45 sec
            Aging Time 45

Interface          Port ID          Designated          Port ID
Name              Prio1Nbr        Cost Sts             Cost Bridge ID      Prio1Nbr
-----
Gi5/4              458165          4 LIS              0 4097 000419b7810800 458165
Gi5/5              458166          4 LIS              0 4097 000419b7810800 458166
Fa4/3              4581495         49 LIS             0 4097 000419b7810800 4581495
Fa4/4              4581496         49 BLK             0 4097 000419b7810800 4581495

Router#
```

[Table 2-85](#) describes the fields that are shown in the example.

**Table 2-85** *show spanning-tree Command Output Fields*

Field	Definition
Port ID Prio.Nbr	Port ID and priority number.
Cost	Port cost.
Sts	Status information.

This example shows how to display information about the spanning tree on active interfaces only:

```
Router# show spanning-tree active
UplinkFast is disabled
BackboneFast is disabled

VLAN4 is executing the ieee compatible Spanning Tree protocol
Bridge Identifier has priority 35768, address 005013e8d16404
Configured hello time 5, max age 50, forward delay 45
Current root has priority 46384, address 00601704c17000
Root port is 565 (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 48:43:54 ago
Times: hold 4, topology change 54, notification 5
      hello 5, max age 44, forward delay 40
Timers: hello 0, topology change 0, notification 0
1
1
1
Router#

```

This example shows how to display the status of spanning-tree BackboneFast:

```

Router# 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
Router#

```

This example shows how to display information about the spanning tree for this bridge only:

```

Router# show spanning-tree bridge
VLAN4
  Bridge ID Priority      35768
           Address      005013e8d16404
           Hello Time   5 sec  Max Age 50 sec  Forward Delay 45 sec
1
1
1
Router#

```

This example shows how to display detailed information about the interface:

```

Router# show spanning-tree detail

VLAN4 is executing the ieee compatible Spanning Tree protocol
Bridge Identifier has priority 4096, address 00d0100b814404
Configured hello time 5, max age 50, forward delay 45
We are the root of the spanning tree
Topology change flag not set, detected flag not set
Number of topology changes 9 last change occurred 05:44:34 ago
from FastEthernet4/54
Times: hold 4, topology change 35, notification 5
hello 5, max age 50, forward delay 45
Timers: hello 4, topology change 0, notification 0, aging 300

Port 543 (FastEthernet4/54) of VLAN4 is forwarding
Port path cost 49, Port priority 458, Port Identifier 45815431
Designated root has priority 4096, address 00d0100b814404
Designated bridge has priority 4096, address 00d0100b814404
Designated port id is 4581543, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 4
BPDU: sent 4845, received 4
Router#

```

This example shows how to display information about the spanning tree for a specific interface:

```
Router# show spanning-tree interface fastethernet 5/9
Interface Fa0/40 (port 53) in Spanning tree 4 is ROOT-INCONSISTENT
Port path cost 400, Port priority 458
Designated root has priority 8495, address 009010c741a400
Designated bridge has priority 35768, address 00e014e9f18940

1
1
1
```

This example shows how to display information about the spanning tree for a specific bridge group:

```
Router# show spanning-tree 1
UplinkFast is disabled
BackboneFast is disabled

Bridge group 4 is executing the ieee compatible Spanning Tree protocol
Bridge Identifier has priority 35768, address 00d01d39c1004d
Configured hello time 5, max age 50, forward delay 45
Current root has priority 35768, address 00d01d39b1fddd
Root port is 7 (FastEthernet5/5), cost of root path is 49
Topology change flag set, detected flag not set
Number of topology changes 3 last change occurred 00:00:04 ago
    from FastEthernet5/5
Times: hold 4, topology change 35, notification 5
    hello 5, max age 50, forward delay 45
Timers: hello 0, topology change 0, notification 0 bridge aging time 45

Port 5 (Ethernet0/4/0) of Bridge group 4 is down

Port path cost 400, Port priority 458
Designated root has priority 35768, address 005010bab14808
Designated bridge has priority 35768, address 005010bab14808
Designated port is 5, path cost 0
Timers: message age 0, forward delay 0, hold 0
BPDU: sent 0, received 0

Router#
```

This example shows how to display a summary of port states:

```
Router# show spanning-tree summary
Root bridge for: Bridge group 4, VLAN0004, VLAN0004-VLAN4005
VLAN4043-VLAN4499, VLAN5004-VLAN4094
EtherChannel misconfiguration guard is enabled
Extended system ID is enabled
Portfast is enabled by default
PortFast BPDU Guard is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard is disabled by default
UplinkFast is disabled
BackboneFast is disabled
Pathcost method used is long
Name                Blocking Listening Learning Forwarding STP Active
-----
4 bridge            0          0          0          4          4
3584 vlans 3584 0 0 7468 40753
                Blocking Listening Learning Forwarding STP Active
-----
Total                3584          0          0          7469          40753
Router#
```

This example shows how to display the total lines of the spanning-tree state section:

```
Router# show spanning-tree summary total
Root bridge for: Bridge group 40, VLAN4, VLAN6, VLAN40001
Extended system ID is enabled1
PortFast BPDU Guard is disabled
EtherChannel misconfiguration guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Default pathcost method used is long

Name                Blocking Listening Learning Forwarding STP Active
-----
405 VLANs 3433      0          0          405        3538

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
Router#
```

This example shows how to display information about the spanning tree for a specific VLAN:

```
Router# show spanning-tree vlan 200
VLAN0500
Spanning tree enabled protocol ieee
Root ID Priority 35768
  Address 00d0100b8144c8
  This bridge is the root
  Hello Time 5 sec Max Age 50 sec Forward Delay 45 sec
Bridge ID Priority 35768
  Address 00d0100b8144c8
  Hello Time 5 sec Max Age 50 sec Forward Delay 45 sec
  Aging Time 300
Interface Role Sts Cost PriolNbr Status
-----
Fa4/4 Desg FWD 500000 4581496 P5p
Fa4/5 Back BLK 500000 4581497 P5p
Router#
```

Table 2-86 describes the fields that are shown in the example.

**Table 2-86** show spanning-tree vlan Command Output Fields

Field	Definition
Role	Current 802.1w role; valid values are Boun (boundary), Desg (designated), Root, Altn (alternate), and Back (backup).
Sts	Spanning-tree states; valid values are BKN* (broken) <sup>1</sup> , BLK (blocking), DWN (down), LTN (listening), LBK (loopback), LRN (learning), and FWD (forwarding).
Cost	Port cost.

**Table 2-86** show spanning-tree vlan Command Output Fields (continued)

Field	Definition
Prio.Nbr	Port ID that consists of the port priority and the port number.
Status	Status information; valid values are as follows: <ul style="list-style-type: none"> <li>• P2p/Shr—The interface is considered as a point-to-point (resp. shared) interface by the spanning tree.</li> <li>• Edge—PortFast has been configured (either globally using the <b>default</b> command or directly on the interface) and no BPDU has been received.</li> <li>• *ROOT_Inc, *LOOP_Inc, *PVID_Inc, and *TYPE_Inc—The port is in a broken state (BKN*) for an inconsistency. The port would be Root inconsistent, Loopguard inconsistent, PVID inconsistent, or Type inconsistent.</li> <li>• Bound(type)—When in MST mode, identifies the boundary ports and specifies the type of the neighbor (STP, RSTP, or PVST).</li> <li>• Peer(STP)—When in PVRST rapid-pvst mode, identifies the port connected to a previous version of the 802.1D bridge.</li> </ul>

1. For information on the \*, see the definition for the Status field.

This example shows how to determine if any ports are in the root-inconsistent state:

```
Router# show spanning-tree inconsistentports
```

```
Name                Interface           Inconsistency
-----
VLAN4                FastEthernet3/4    Root Inconsistent
```

```
Number of inconsistent ports (segments) in the system :4
Router#
```

#### Related Commands

Command	Description
<a href="#">spanning-tree backbonefast</a>	Enables BackboneFast on all Ethernet VLANs.
<a href="#">spanning-tree cost</a>	Sets the path cost of the interface for STP calculations.
<a href="#">spanning-tree guard</a>	Enables or disables the guard mode.
<a href="#">spanning-tree pathcost method</a>	Sets the default path-cost calculation method.
<a href="#">spanning-tree portfast (interface configuration mode)</a>	Enables PortFast mode.
<a href="#">spanning-tree portfast bpdupfilter default</a>	Enables BPDU filtering by default on all PortFast ports.
<a href="#">spanning-tree portfast bpduguard default</a>	Enables BPDU guard by default on all PortFast ports.
<a href="#">spanning-tree port-priority</a>	Sets an interface priority when two bridges vie for position as the root bridge.
<a href="#">spanning-tree uplinkfast</a>	Enables UplinkFast.
<a href="#">spanning-tree vlan</a>	Configures STP on a per-VLAN basis.

## show spanning-tree mst

To display the information about the MST protocol, use the **show spanning-tree mst** command.

```
show spanning-tree mst [configuration [digest]]
```

```
show spanning-tree mst [instance-id] [detail]
```

```
show spanning-tree mst [instance-id] interface interface [detail]
```

Syntax Description	
<b>configuration</b>	(Optional) Displays information about the region configuration.
<b>digest</b>	(Optional) Displays information about the MD5 digest included in the current MSTCI.
<i>instance-id</i>	(Optional) Instance identification number; valid values are from 0 to 4094.
<b>detail</b>	(Optional) Displays detailed information about the MST protocol.
<b>interface interface</b>	(Optional) Displays the interface type and number; possible valid values for type are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , <b>atm</b> , <b>ge-wan</b> , <b>port-channel</b> , and <b>vlan</b> . See the “Usage Guidelines” section for valid number values.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The valid values for *interface* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 2 to 13 and valid values for the port number are from 1 to 48.

The number of valid values for **port-channel number** are a maximum of 64 values ranging from 1 to 282. The **port-channel number** values from 257 to 282 are supported on the CSM and the FWSM only.

The number of valid values for **vlan** are from 1 to 4094.

Valid values for *instance-id* are from 0 to 4094.

In the output display of the **show spanning-tree mst configuration** command, a warning message may display. This message appears if you do not map secondary VLANs to the same instance as the associated primary VLAN. The display includes a list of the secondary VLANs that are not mapped to the same instance as the associated primary VLAN. The warning message is as follows:

```
These secondary vlans are not mapped to the same instance as their primary:
-> 3
```

In the output display of the **show spanning-tree mst configuration digest** command, if the output applies to both standard and prestandard bridges at the same time on a per-port basis, two different digests are displayed.

If you configure a port to transmit prestandard BPDUs only, the prestandard flag displays in the **show spanning-tree** commands. The variations of the prestandard flag are as follows:

- Pre-STD (or prestandard in long format)—This flag displays if the port is configured to transmit prestandard BPDUs and if a prestandard neighbor bridge has been detected on this interface.
- Pre-STD-Cf (or prestandard (config) in long format)—This flag displays if the port is configured to transmit prestandard BPDUs but a prestandard BPDU has not been received on the port, the autodetection mechanism has failed, or a misconfiguration, if there is no prestandard neighbor, has occurred.
- Pre-STD-Rx (or prestandard (rcvd) in long format)—This flag displays when a prestandard BPDU has been received on the port but it has not been configured to send prestandard BPDUs. The port will send prestandard BPDUs, but we recommend that you change the port configuration so that the interaction with the prestandard neighbor does not rely only on the autodetection mechanism.

If the configuration is not prestandard compliant (for example, a single MST instance has an ID that is greater than or equal to 16), the prestandard digest is not computed and the following output is displayed:

```
Router# show spanning-tree mst configuration digest
Name      [region4]
Revision  5      Instances configured 3
Digest    0x3C60DBF54B03EBF09C5955F456D48A03
Pre-std Digest  N/A, configuration not pre-standard compatible
Router#
```

MST BPDUs include an MST configuration identifier (MSTCI) that consists of the region name, region revision, and an MD5 digest of the VLAN-to-instance mapping of the MST configuration.

See the **show spanning-tree** command for output definitions.

## Examples

This example shows how to display information about the region configuration:

```
Router> show spanning-tree mst configuration
Name      [leo]
Revision  5705
Instance  Vlans mapped
-----
0         4-9,44-49,54-59,34-39,44-4094
4         40,50,30,40
-----
```

This example shows how to display additional MST-protocol values:

```
Router# show spanning-tree mst 3 detail
##### MST03 vlans mapped: 3,3000-3999
Bridge address 00051475c1f400 priority 35774 (35768 sysid 3)
Root this switch for MST03
```

```
GigabitEthernet4/4 of MST03 is boundary forwarding
Port info port id 45814 priority 458
cost 50000
Designated root address 00051475c1f400 priority 35774
cost 0
Designated bridge address 00051475c1f400 priority 35774 port
id 45814
Timers: message expires in 0 sec, forward delay 0, forward transitions 4
Bpdus (MRecords) sent 4, received 0

FastEthernet4/4 of MST03 is designated forwarding
Port info port id 4581493 priority 458 cost
500000
Designated root address 00051475c1f400 priority 35774
cost 0
Designated bridge address 00051475c1f400 priority 35774 port id
4581493
Timers: message expires in 0 sec, forward delay 0, forward transitions 4
Bpdus (MRecords) sent 554, received 4

FastEthernet4/5 of MST03 is backup blocking
Port info port id 4581494 priority 458 cost
500000
Designated root address 00051475c1f400 priority 35774
cost 0
Designated bridge address 00051475c1f400 priority 35774 port id
4581493
Timers: message expires in 5 sec, forward delay 0, forward transitions 4
Bpdus (MRecords) sent 3, received 555
Router#
```

This example shows how to display MST information for a specific interface:

```
Router# show spanning-tree mst 0 interface fastethernet 4/1 detail
Edge port: no (trunk) port guard : none
(default)
Link type: point-to-point (point-to-point) bpdu filter: disable
(default)
Boundary : internal bpdu guard : disable
(default)
FastEthernet4/4 of MST00 is designated forwarding
Vlans mapped to MST00 4-5,4-5999,4000-4094
Port info port id 4581493 priority 458 cost
500000
Designated root address 005013e661d000 priority 8493
cost 50004
Designated ist master address 00051475c1f400 priority 49455
cost 0
Designated bridge address 00051475c1f400 priority 49455 port id
4581493
Timers: message expires in 0 sec, forward delay 0, forward transitions 4
Bpdus sent 495, received 3
Router#
```

This example shows how to display the MD5 digest included in the current MSTCI:

```
Router# show spanning-tree mst configuration digest
Name      [mst-config]
Revision  40      Instances configured 55
Digest    0x40D5ECA478C657835C83BBCB46753495
Pre-std Digest 0x57BF445A75B75784ED958D9EC5BB4554
Router#
```

This example displays the new master role for all MST instances at the boundary of the region on the port that is a CIST root port:

```
Router# show spanning-tree mst interface fastethernet4/9

FastEthernet4/9 of MST00 is root forwarding
Edge port: no (default) port guard : none (default)
Link type: point-to-point (auto) bpdu filter: disable (default)
Boundary : boundary (RSTP) bpdu guard : disable (default)
Bpdus sent 3458, received 6774

Instance Role Sts Cost PriolNbr Vlans mapped
-----
0 Root FWD 500000 4581504 5-7,40,45-99,404-999,5004-3999,4004-4094
8 Mstr FWD 500000 4581504 8,4000
9 Mstr FWD 500000 4581504 4,9,400
44 Mstr FWD 500000 4581504 44,4000-5000
Router#
```

#### Related Commands

Command	Description
<a href="#">spanning-tree mst</a>	Sets the path cost and port-priority parameters for any MST instance.
<a href="#">spanning-tree mst forward-time</a>	Sets the forward-delay timer for all the instances on the Catalyst 6500 series switch.
<a href="#">spanning-tree mst hello-time</a>	Sets the hello-time delay timer for all the instances on the Catalyst 6500 series switch.
<a href="#">spanning-tree mst max-hops</a>	Specifies the number of possible hops in the region before a BPDU is discarded.
<a href="#">spanning-tree mst root</a>	Designates the primary and secondary root, sets the bridge priority, and sets the timer value for an instance.

# show standby delay

To display HSRP information about the delay periods, use the **show standby delay** command.

**show standby delay** [*type number*]

<b>Syntax Description</b>	<i>type number</i> (Optional) Interface type and number for which output is displayed.
---------------------------	--

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display information about the delay periods:

```
Router# show standby delay

Interface           Minimum Reload
Ethernet0/3         4             5
Router#
```

Related Commands	Command	Description
	<a href="#">standby delay</a>	Configures the delay period before the initialization of HSRP groups.
	<a href="#">minimum reload</a>	

# show sup-bootflash

To display information about the sup-bootflash file system, use the **show sup-bootflash** command.

**show sup-bootflash** [**all** | **chips** | **fileSYS**]

Syntax Description	all	(Optional) Displays all possible flash information.
	<b>chips</b>	(Optional) Displays information about the flash chip.
	<b>fileSYS</b>	(Optional) Displays information about the file system.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display a summary of bootflash information:

```
Router# show sup-bootflash
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
4  11 image    EBC8FC4D  A7487C   6 40700796 Nov 49 4999 07:07:37 halley
5  11 unknown  C7EB077D  EE5650  55 4644430 Nov 49 4999 07:50:44 cat6000-sup_
5-3-3-CSX1bin

645600 bytes available (45345484 bytes used)
Router#
```

This example shows how to display all bootflash information:

```
Router# show sup-bootflash all
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
4  11 image    EBC8FC4D  A7487C   6 40700796 Nov 49 4999 07:07:37 halley
5  11 unknown  C7EB077D  EE5650  55 4644430 Nov 49 4999 07:50:44 cat6000-sup_
5-3-3-CSX1bin

645600 bytes available (45345484 bytes used)

----- F I L E   S \ S T E M   S T A T U S -----
Device Number = 5
DEVICE INFO BLOCK: bootflash
  Magic Number          = 6887635   File System Vers = 40000   (410)
  Length                = 4000000   Sector Size      = 40000
  Programming Algorithm = 49        Erased State     = FFFFFFFF
  File System Offset    = 40000    Length = F40000
  MONLIB Offset        = 400        Length = F568
  Bad Sector Map Offset = 3FFF8    Length = 8
  Squeeze Log Offset   = F80000    Length = 40000
  Squeeze Buffer Offset = FC0000    Length = 40000
  Num Spare Sectors    = 0
```

```

    Spares:
STATUS INFO:
  Writable
  NO File Open for Write
  Complete Stats
  No Unrecovered Errors
  No Squeeze in progress
USAGE INFO:
  Bytes Used      = EA5650  Bytes Available = 9D9E0
  Bad Sectors    = 0        Spared Sectors  = 0
  OK Files       = 5        Bytes = EA5550
  Deleted Files  = 0        Bytes = 0
  Files w/Errors = 0        Bytes = 0

```

```
***** Intel SCS Status/Register Dump *****
```

```
COMMON MEMOR\ REGISTERS: Bank 0
  Intelligent ID Code : 890089
  Compatible Status Reg: 800080
```

```
DEVICE T\PE:
  Layout           : Paired x46 Mode
  Write Queue Size : 64
  Queued Erase Supported : No
```

```
Router#
```

This example shows how to display information about the flash chip:

```
Router# show sup-bootflash chips
```

```
***** Intel SCS Status/Register Dump *****
```

```
COMMON MEMOR\ REGISTERS: Bank 0
  Intelligent ID Code : 890089
  Compatible Status Reg: 800080
```

```
DEVICE T\PE:
  Layout           : Paired x46 Mode
  Write Queue Size : 64
  Queued Erase Supported : No
```

```
Router#
```

This example shows how to display information about the file system:

```
Router# show sup-bootflash filesystems
```

```

----- F I L E   S \ S T E M   S T A T U S -----
  Device Number = 5
DEVICE INFO BLOCK: bootflash
  Magic Number      = 6887635  File System Vers = 40000  (410)
  Length           = 4000000  Sector Size     = 40000
  Programming Algorithm = 49    Erased State    = FFFFFFFF
  File System Offset = 40000   Length = F40000
  MONLIB Offset     = 400     Length = F568
  Bad Sector Map Offset = 3FFF8  Length = 8
  Squeeze Log Offset = F80000  Length = 40000
  Squeeze Buffer Offset = FC0000  Length = 40000
  Num Spare Sectors = 0
    Spares:
STATUS INFO:
  Writable
  NO File Open for Write

```

```
Complete Stats
No Unrecovered Errors
No Squeeze in progress
USAGE INFO:
  Bytes Used      = EA5650  Bytes Available = 9D9E0
  Bad Sectors    = 0        Spared Sectors = 0
  OK Files       = 5        Bytes = EA5550
  Deleted Files  = 0        Bytes = 0
  Files w/Errors = 0        Bytes = 0
```

```
Router#
```

# show system jumbomtu

To display the global MTU setting, use the **show system jumbomtu** command.

**show system jumbomtu**

---

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

---

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

---

**Command Modes** Privileged EXEC

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Examples** This example shows how to display the global MTU setting:

```
Router# show system jumbomtu
Global Ethernet MTU is 4550 bytes1
Router#
```

---

Related Commands	Command	Description
	<a href="#">system jumbomtu</a>	Sets the maximum size of the Layer 2 and Layer 3 packets.

---

# show tcam counts

To display the TCAM statistics, use the **show tcam counts** command.

**show tcam counts** [*module number*]

Syntax Description	<b>module number</b>	(Optional) Specifies the module number; see the “Usage Guidelines” section for valid values.
--------------------	----------------------	--

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **module number** keyword and argument designate the module and port number. Valid values for *number* depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 2 to 13 and valid values for the port number are from 1 to 48.

**Examples** This example shows how to display the TCAM statistics:

```
Router# show tcam counts
          Used      Free      Percent Used      Reserved
          ----      ----      -
Labels:      8      504      4
ACL_TCAM
-----
Masks:      6      4090      0      0
Entries:    37      35734      0      0
QOS_TCAM
-----
Masks:      3      4093      0      0
Entries:    50      35748      0      0
LOU:        0      458      0
ANDOR:      0      46      0
ORAND:      0      46      0
ADJ:        4      5047      0
Router#
```

Table 2-87 describes the fields that are shown in the example.

**Table 2-87** *show tcam counts Command Output Fields*

Field	Description
Labels Used	Number of labels that are used (maximum of 512).
Labels Free	Number of free labels remaining.
Labels Percent Used	Percentage of labels that are used.
Masks Used	Number of masks that are used (maximum of 4096).
Masks Free	Number of free labels remaining.
Masks Percent Used	Percentage of masks that are used.
Entries Used	Number of labels that are used (maximum of 32767).
Entries Free	Number of free labels that are remaining.
Entries Percent Used	Percentage of entries that are used.

# show tcam interface

To display information about the interface-based TCAM, use the **show tcam interface** command.

```
show tcam interface {interface interface-number} | {null interface-number} | {vlan vlan-id} {acl
{in | out}} | {qos {type1 | type2}} type [detail | module number]
```

Syntax Description	
<i>interface</i>	(Optional) Interface type; possible valid values are <b>ethernet</b> , <b>fastethernet</b> , <b>gigabitethernet</b> , <b>tengigabitethernet</b> , <b>pos</b> , <b>atm</b> , and <b>ge-wan</b> .
<i>interface-number</i>	(Optional) Module and port number; see the “Usage Guidelines” section for valid values.
<b>null</b> <i>interface-number</i>	(Optional) Specifies the null interface; the valid value is <b>0</b> .
<b>vlan</b> <i>vlan-id</i>	(Optional) Specifies the VLAN; see the “Usage Guidelines” section for valid values.
<b>acl in</b>	(Optional) Displays the ACL-based incoming packets.
<b>acl out</b>	(Optional) Displays the ACL-based outgoing packets.
<b>qos type1</b>	(Optional) Displays the QoS-based Type 1 packets.
<b>qos type2</b>	(Optional) Displays the QoS-based Type 2 packets.
<i>type</i>	Protocol type to display; valid values are <b>arp</b> , <b>ipv4</b> , <b>ipv6</b> , <b>mpls</b> , and <b>other</b> .
<b>detail</b>	(Optional) Displays detailed information.
<b>module</b> <i>number</i>	(Optional) Specifies the module number.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Use the **clear mls acl counters** command to clear the TCAM ACL match counters.

**Examples**

This example shows how to display interface-based TCAM information:

```
Router# show tcam interface vlan 7 acl in ip
deny ip any any
permit ip 501501010 01015551555 551551010 01015551555
redirect ip 501541010 01015551555 551531010 01015551555
permit tcp 541541010 01015551555 301301010 01015551555
Fragments (4 match)
permit tcp 551551010 01015551555 341341010 01015551555
fragments
permit tcp 551551010 01015551555 range 30000 30050 341341010
01015551555 range 40000 40040 (405 matches)
permit tcp 541541010 01015551555 eq 9000 301301010 01015551555
eq telnet
deny ip any any
deny ip any any
Router#
```

This example shows how to display detailed TCAM information:

```
Router# show tcam interface fa5/2 acl in ip detail
```

```
-----
-----
DPort - Destination Port   SPort - Source Port       TCP-F - U -URG
Pro   - Protocol
I     - Inverted LOU       TOS   - TOS Value           - A -ACK
rtr   - Router
MRFM  - M -MPLS Packet    TN    - T -Tcp Control         - P -PSH
COD   - C -Bank Care Flag
      - R -Recirc1 Flag    - N   -Non-cachable       - R -RST
      - I -OrdIndepl Flag
      - F -Fragment Flag   CAP   - Capture Flag          - S -S\N
      - D -Dynamic Flag
      - M -More Fragments  F-P   - FlowMask-Prior1      - F -FIN
T     - V(Value)/M(Mask)/R(Result)
X     - XTAG               (*)   - Bank Priority
-----
-----
```

```
Interface: 4048   label: 4   lookup_type: 0
protocol: IP     packet-type: 0
```

```
+-----+-----+-----+-----+-----+-----+
+---+---+---+---+---+---+
;T;Index;  Dest Ip Addr ; Source Ip Addr;   DPort   ;   SPort   ; TCP-F
;Pro;MRFM;X;TOS;TN;COD;F-P;
+-----+-----+-----+-----+-----+-----+
+---+---+---+---+---+---+
V 48396      0101010      0101010      P=0      P=0      -----
  0 ---- 0   0 -- --- 0-0
M 48404      0101010      0101010      0        0
```

```

0 ---- 0 0
R rslt: L3_DEN\_RESULT          rtr_rslt: L3_DEN\_RESULT

V 36858          0101010      0101010      P=0          P=0      -----
0 ---- 0 0 -- --- 0-0
M 36836          0101010      0101010      0            0
0 ---- 0 0
R rslt: L3_DEN\_RESULT (*)      rtr_rslt: L3_DEN\_RESULT (*)
Router#

```

**Related Commands**

Command	Description
<a href="#">clear mls acl counters</a>	Clears the MLS ACL counters.

# show tech-support

To display information that is useful to Cisco TAC when reporting a problem, use the **show tech-support** command.

```
show tech-support [cef | ipmulticast [vrf instance-number] | isis | password [page] | platform |
page | rsvp]
```

Syntax Description		
<b>cef</b>	(Optional)	Displays CEF-related TAC information.
<b>ipmulticast</b>	(Optional)	Displays IP multicast-related TAC information.
<b>vrf</b> <i>instance-number</i>	(Optional)	Specifies an VRF instance number.
<b>isis</b>	(Optional)	Displays CLNS- and ISIS-related TAC information.
<b>password</b>	(Optional)	Removes passwords and other security information in the output.
<b>page</b>	(Optional)	Causes the output to display a page of information at a time.
<b>platform</b>	(Optional)	Displays platform-specific TAC information.
<b>rsvp</b>	(Optional)	Displays IP RSVP-related TAC information.

## Defaults

The defaults are as follows:

- Outputs are displayed without page breaks.
- Passwords and other security information are removed from the output.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

To interrupt and terminate the **show tech-support** output, simultaneously press and release the **CTRL**, **ALT**, and **6** keys.

Press the **Return** key to display the next line of output, or press the **Space** bar to display the next page of information. If you do not enter the **page** keyword, the output scrolls (that is, it does not stop for page breaks).

If you do not enter the **password** keyword, passwords and other security-sensitive information in the output are replaced with the label “<removed>.”

The **show tech-support** commands are a compilation of several **show** commands and can be lengthy. For a sample display of the output of the **show tech-support** command, see the individual **show** command listed.

If you enter the **show tech-support** command without arguments, the output displays, but is not limited to, the equivalent of these **show** commands:

- **show version**
- **show running-config**
- **show stacks**
- **show interfaces**
- **show controllers**
- **show process memory**
- **show process cpu**
- **show buffers**
- **show logging**
- **show module**
- **show power**
- **show environment**
- **show interfaces switchport**
- **show interfaces trunk**
- **show vlan**
- **show mac-address-table**
- **show spanning-tree**

If you enter the **ipmulticast** keyword, the output displays, but is not limited to, these **show** commands:

- **show ip pim interface**
- **show ip pim interface count**
- **show ip pim interface df**
- **show ip pim mdt**
- **show ip pim mdt bgp**
- **show ip pim neighbor**
- **show ip pim rp**
- **show ip pim rp metric**
- **show ip igmp groups**
- **show ip igmp interface**
- **show mls ip multicast rp-mapping gm-cache**
- **show ip mroute count**
- **show ip mroute**
- **show ip mcache**
- **show ip dvmrp route**
- **show mmls msc rpdf-cache**
- **show mmls gc process**

## ■ show tech-support

If you enter the **isis** keyword, the output displays the equivalent of the **show isis** commands.

If you enter the **rsvp** keyword, the output displays the equivalent of the **show ip rsvp** commands.

---

**Examples**

For a sample display of the **show tech-support** command output, see the commands that are listed in the “Usage Guidelines” section.

# show top counters interface report

To display TopN reports and information, use the **show top counters interface report** command.

**show top counters interface report** [*number*]

<b>Syntax Description</b>	<i>number</i> (Optional) Number of the report to be displayed; valid values are from 1 to 5.
---------------------------	--

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	This command is supported on Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet ports only.
-------------------------	---

When you enter a TopN request, a round of polling is performed, the counters for all the applicable ports in the Catalyst 6500 series switch are read, and the information is saved. The TopN process then sleeps for the specified interval. After wakeup, another round of polling is performed and the counter information from the ports is read. The difference between the two sets of data is stored. The ports are then sorted, the ports choose from one of the seven types of statistics information, and a TopN report is generated.

The port statistics will not be displayed in the following cases:

- If a port is not present during the first poll.
- If a port is not present during the second poll.
- If a port's speed or duplex changes during the polling interval.
- If a port's type changes from Layer 2 to Layer 3 or Layer 3 to Layer 2 during the polling interval.



<b>Note</b>	For the report display format, due to the 80 characters per line limitation, only 10 spaces are reserved for the <i>Tx/Rx-okts</i> , <i>Tx/Rx-bcst</i> , and <i>Tx/Rx-mcst</i> columns. When these columns are larger than 10 digits, the display wraps around to the next line.
-------------	--

When you start the TopN processes from a Telnet session and the Telnet session is terminated before the TopN processes are completed, all the background TopN processes continue and generate the TopN reports, but the foreground TopN processes are terminated once the Telnet session is terminated.

When the TopN report is being generated against a large number of ports (for example, 13 slot x 96 ports/slot) in a very short interval (10 seconds), the actual interval time between the first and second polling may be longer than the specified interval time because polling takes time.

**Examples**

This example shows how to display TopN reports and information:

```
Router# show top counters interface report
Id Start Time                Int N   Sort-By   Status   Owner
-----
4  08:48:55 UTC Tue Nov 53 5004 76  50  util     done    console
5  08:49:54 UTC Tue Nov 53 5004 76  50  util     done    console
3  08:54:34 UTC Tue Nov 53 5004 76  50  util     done    console
4  08:56:50 UTC Tue Nov 53 5004 90  50  util     done    bambam onvty0 (9140169143)
Router#
```

This example shows how to display TopN reports and information for a specific report:

```
Router# show top counters interface report 1
Started By      : console
Start Time     : 08:48:55 UTC Tue Nov 53 5004
End Time       : 08:49:45 UTC Tue Nov 53 5004
Port Type      : All
Sort By        : util
Interval       : 76 seconds
Port   Band  Util Bytes      Packets      Broadcast  Multicast  In-  Buf-
      width  (Tx + Rx)  (Tx + Rx)    (Tx + Rx)  (Tx + Rx)  err  ovflw
-----
Fa5/5  400   50  756047564  44344488    44344487   4         0     0
Fa5/48 400   35  508048905  7937789     0          43        0     0
Fa5/46 400   55  365860697  5669693     0          43        0     0
Fa5/47 400   55  353855889  4765539     4765495    43        0     0
Fa5/6  400   45  547845835  3403375     0          39        54    0
Fa5/44 400   40  445446009  5567900     0          43        0     0
Gi4/45 4000  0   0           0           0           0         0     0
Gi4/44 4000  0   0           0           0           0         0     0
Gi4/43 4000  0   0           0           0           0         0     0
Gi4/45 4000  0   0           0           0           0         0     0
Gi4/44 4000  0   0           0           0           0         0     0
Gi4/40 4000  0   0           0           0           0         0     0
Gi4/9  4000  0   0           0           0           0         0     0
Gi4/8  4000  0   776         5           0           5         0     0
Gi4/7  4000  0   0           0           0           0         0     0
Gi4/6  4000  0   0           0           0           0         0     0
Gi4/5  4000  0   0           0           0           0         0     0
Gi4/4  4000  0   0           0           0           0         0     0
Gi4/3  4000  0   776         5           0           5         0     0
Gi4/5  4000  0   0           0           0           0         0     0
Router#
```

This example shows the display if you request a TopN report that is still in pending status:

```
Router# show top counters interface report 4
Id  Start time                Int N   Sort-by   Status   Owner (type/machine/user)
-----
4  4/54/5004,44:34:56  30  50  In-Errors  pending  Console//
Router#
```

**Related Commands**

Command	Description
<a href="#">clear top counters interface report</a>	Clears the TopN reports.
<a href="#">collect top counters interface</a>	Lists the TopN processes and specific TopN reports.

# show uddl

To display the administrative and operational UDLD status, use the **show uddl** command.

**show uddl** [*interface-id* | **neighbors**]

Syntax Description	
<i>interface-id</i>	(Optional) Interface name.
<b>neighbors</b>	(Optional) Displays neighbor information only.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** If you do not enter an *interface-id* value, the administrative and operational UDLD status for all interfaces is displayed.

**Examples** This example shows how to display the UDLD state for a single interface:

```
Router# show uddl gigabitethernet2/2

Interface Gi5/5
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement
Message interval: 60
Time out interval: 5
No multiple neighbors detected
  Entry 4
  ---
  Expiration time: 446
  Device ID: 4
  Current neighbor state: Bidirectional
  Device name: 0050e5856000
  Port ID: 5/4
  Neighbor echo 4 device: SAD03460954
  Neighbor echo 4 port: Gi4/4

  Message interval: 5
  CDP Device name: 066557794
Router#
```

This example shows how to display neighbor information only:

## ■ show udd

```

Router# show udd neighbors
Port      Device Name                Device ID  Port-ID  OperState
-----
Gi3/4     SAL0734K5R5                4         Gi4/4    Bidirectional
Gi4/4     SAL0734K5R5                4         Gi3/4    Bidirectional
Router#

```

---

**Related Commands**

Command	Description
<b>udd</b>	Enables aggressive or normal mode in UDLD and sets the configurable message time.
<b>udd port</b>	Enables UDLD on the interface or enables UDLD in aggressive mode on the interface.

# show version

To display the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images, use the **show version** command.

## show version

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

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images:

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) c6sup5_rp Software (c6sup5_rp-JSV-M), Version 4514(nightly1E050656) NIG
HTL\ BUILD
Copyright (c) 4986-5005 by cisco Systems, Inc1
Compiled Wed 56-Jun-05 06:50 by
Image text-base: 0x40008BF0, data-base: 0x449BA000

ROM: System Bootstrap, Version 4514(44r)E4, RELEASE SOFTWARE (fc4)

Router uptime is 5 weeks, 8 hours, 48 minutes
Time since Router switched to active is 4 minute
System returned to ROM by power-on (SP by power-on)
System image file is "sup-bootflash:c6sup55-jsv-mz"

cisco Catalyst 6000 (R7000) processor with 445640K/48435K bytes of memory1
Processor board ID SAD06540067
R7000 CPU at 300Mhz, Implementation 39, Rev 313, 556KB L5, 4054KB L3 Cache
Last reset from power-on
Bridging software1
X155 software, Version 310101
SuperLAT software (copyright 4990 by Meridian Technology Corp)1
TN3570 Emulation software1
3 Virtual Ethernet/IEEE 80513 interface(s)
48 FastEthernet/IEEE 80513 interface(s)
384K bytes of non-volatile configuration memory1

46384K bytes of Flash internal SIMM (Sector size 545K)1
Configuration register is 0x5405
Router#
```

Table 2-88 describes the fields that are shown in the example.

**Table 2-88** *show version Field Descriptions*

Field	Description
IOS (tm) c6sup2_rp Software (c6sup2_rp-JSV-M), Version 12.1(nightly.E020626) NIGHTLY BUILD	Version number. Always specify the complete version number when reporting a possible software problem. In the example output, the version number is 12.1.
ROM: System Bootstrap, Version 12.1(11r)E1, RELEASE SOFTWARE (fc1)	Bootstrap version string.
BOOTFLASH: 7200 Software (C7200-BOOT-M), Version 11.1(472), RELEASE SOFTWARE	Boot version string.
Router uptime is	Amount of time that the system has been up and running.
Time since Router switched to active	Amount of time since switchover occurred.
System restarted by	Log of how the system was last booted, both as a result of normal system startup and of system error. For example, information can be displayed to indicate a bus error that is typically the result of an attempt to access a nonexistent address, as follows:  System restarted by bus error at PC 0xC4CA, address 0x210C0C0
System image file is	If the software was booted over the network, the Internet address of the boot host is shown. If the software was loaded from onboard ROM, this line reads “running default software.”
cisco Catalyst 6000 (R7000) processor with 112640K/18432K bytes of memory.	Remaining output in each display that shows the hardware configuration and any nonstandard software options.
Configuration register is	Configuration register contents that are displayed in hexadecimal notation.

The output of the **show version EXEC** command can provide certain messages, such as bus error messages. If such error messages appear, report the complete text of this message to your technical support specialist.

# show vlan

To display VLAN information, use the **show vlan** command.

```
show vlan [{brief | {id vlan-id} | {name name} [ifindex]} | ifindex]
```

Syntax Description		
<b>brief</b>	(Optional)	Displays only a single line for each VLAN, naming the VLAN, status, and ports.
<b>id</b> <i>vlan-id</i>	(Optional)	Displays information about a single VLAN that is identified by a VLAN ID number; valid values are from 1 to 4094.
<b>name</b> <i>name</i>	(Optional)	Displays information about a single VLAN that is identified by VLAN name; valid values are an ASCII string from 1 to 32 characters.
<b>ifindex</b>	(Optional)	Displays the VLAN's ifIndex number.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Each Ethernet switch port and Ethernet repeater group belong to only one VLAN. Trunk ports can be on multiple VLANs.

If you shut down a VLAN using the **state suspend** or the **state active** command, these values appear in the Status field:

- suspended—VLAN is suspended.
- active—VLAN is active.

If you shut down a VLAN using the **shutdown** command, these values appear in the Status field:

- act/ishut—VLAN status is active but shut down locally.
- sus/ishut—VLAN status is suspended but shut down locally.

If a VLAN is shut down internally, these values appear in the Status field:

- act/ishut—VLAN status is active but shut down internally.
- sus/ishut—VLAN status is suspended but shut down internally.

If a VLAN is shut down locally and internally, the value that is displayed in the Status field is act/ishut or sus/ishut. If a VLAN is shut down locally only, the value that is displayed in the Status field is act/ishut or sus/ishut.

Separate VLAN ranges with a hyphen, and separate VLANs with a comma and no spaces in between. For example, you can enter the following:

```
Router# show vlan id 1-4,3,7,5-20
```

**Examples**

This example shows the output for a VLAN (VLAN0002) that is active but shut down internally:

```
Router# show vlan
VLAN Name                Status    Ports
-----
4    default                active    Fa5/9
5    VLAN0005              act/ishut Fa5/9
<111Output truncated111>
```

This example shows the output for a VLAN (VLAN0002) that is active but shut down locally:

```
Router# show vlan
VLAN Name                Status    Ports
-----
4    default                active    Fa5/9
5    VLAN0005              act/lshut Fa5/9
<111Output truncated111>
```

This example shows how to display the VLAN parameters for all VLANs within the administrative domain:

```
Router# show vlan
VLAN Name                Status    Ports
-----
4    default                active    Fa5/9
5    VLAN0005              active    Fa5/9
3    VLAN0003              active    Fa5/9
4    VLAN0004              active    Fa5/9
5    VLAN0005              active    Fa5/9
6    VLAN0006              active    Fa5/9
<111Output truncated111>

4004 fddinet-default      active    Fa5/9
4005 trbrf-default       active    Fa5/9

VLAN Type  SAID      MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans4 Trans5
-----
4    enet     400004   4500  -     -     -     -     -         0      0
5    enet     400005   4500  -     -     -     -     -         0      0
3    enet     400003   4500  -     -     -     -     -         303    0
4    enet     400004   4500  -     -     -     -     -         304    0
5    enet     400005   4500  -     -     -     -     -         305    0
6    enet     400006   4500  -     -     -     -     -         0      0
40   enet     400040   4500  -     -     -     -     -         0      0
<111Output truncated111>

Remote SPAN VLANs
-----
5, 50

Primary Secondary Type          Ports
-----
Router#
```

This example shows how to display the VLAN name, status, and associated ports only:

```
Router# show vlan brief
VLAN Name                Status    Ports
-----
4    default                active    Fa5/9
5    VLAN0005              active    Fa5/9
3    VLAN0003              act/lshut Fa5/9
4    VLAN0004              act/lshut Fa5/9
```

```

5    VLAN0005                active    Fa5/9
40   VLAN0040                active    Fa5/9
1
1
1
999  VLAN0999                active    Fa5/9
4005 fddi-default            active    Fa5/9
4003 trcrf-default          active    Fa5/9
4004 fddinet-default        active    Fa5/9
4005 trbrf-default          active    Fa5/9
Router#

```

This example shows how to display the VLAN parameters for multiple VLANs:

```
Router# show vlan id 1-4,3,7,5-20
```

VLAN	Name	Status	Ports
4	default	active	Fa5/7, Fa5/45
5	VLAN0005	active	
3	VLAN0003	act/lshut	
4	VLAN0004	act/lshut	
5	VLAN0005	active	
6	VLAN0006	active	
40	VLAN0040	active	
50	VLAN0050	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans4	Trans5
4	enet	400004	4500	-	-	-	-	-	0	0
5	enet	400005	4500	-	-	-	-	-	0	0
3	enet	400003	4500	-	-	-	-	-	303	0
4	enet	400004	4500	-	-	-	-	-	304	0
5	enet	400005	4500	-	-	-	-	-	305	0
6	enet	400006	4500	-	-	-	-	-	0	0
40	enet	400040	4500	-	-	-	-	-	0	0
50	enet	400050	4500	-	-	-	-	-	0	0

Remote SPAN VLANs

Primary	Secondary	Type	Ports

```
Router#
```

This example shows how to display the ifIndex number for VLAN 10 only:

```
Router# show vlan id 10 ifindex
```

```

VLAN Ifindex
-----
40    37
Router#

```

Table 2-89 describes the fields that are shown in the example.

**Table 2-89 show vlan Command Output Fields**

Field	Description
VLAN	VLAN number.
Name	Name, if configured, of the VLAN.
Status	Status of the VLAN (active or suspend, act/lshut or sus/lshut, or act/ishut or sus/ishut).
Ports	Ports that belong to the VLAN.
Type	Media type of the VLAN.
SAID	Security association ID value for the VLAN.
MTU	Maximum transmission unit size for the VLAN.
Parent	Parent VLAN, if one exists.
RingNo	Ring number for the VLAN, if applicable.
BrdgNo	Bridge number for the VLAN, if applicable.
Stp	Spanning Tree Protocol type that is used on the VLAN.
BrdgMode	Bridging mode for this VLAN—possible values are SRB and SRT; the default is SRB.
AREHops	Maximum number of hops for All-Routes Explorer frames—possible values are 1 through 13; the default is 7.
STEHops	Maximum number of hops for Spanning Tree Explorer frames—possible values are 1 through 13; the default is 7.
Backup CRF	Status of whether the TrCRF is a backup path for traffic.
Ifindex	Number of the ifIndex.
Remote SPAN VLAN	RSPAN status.
Primary	Number of the primary VLAN.
Secondary	Number of the secondary VLAN.
Ports	Indicates the ports within a VLAN.
Type	Type of VLAN—Possible values are primary, isolated, community, nonoperation, or normal.

#### Related Commands

Command	Description
<a href="#">show vlan private-vlan</a>	Displays PVLAN information.
<a href="#">vlan (config-VLAN submode)</a>	Configures a specific VLAN.
<a href="#">vtp</a>	Configures the global VTP state.

# show vlan access-log

To display information about the VACL logging including the configured logging properties, flow table contents, and statistics, use the **show vlan access-log** command.

## show vlan access-log config

```
show vlan access-log flow protocol {{src-addr src-mask} | any | {host {hostname | host-ip}}}  
                                {{dst-addr dst-mask} | any | {host {hostname | host-ip}} } [vlan vlan-id]
```

## show vlan access-log statistics

Syntax	Description
<b>config</b>	Displays the configured VACL-logging properties.
<b>flow</b>	Displays the contents of the VACL-flow table.
<i>protocol</i>	Protocol name or number; valid values are <b>icmp</b> , <b>igmp</b> , <b>ip</b> , <b>tcp</b> , <b>udp</b> , or numbers from 0 to 255 to designate a protocol.
<i>src-addr src-mask</i>	Source address and mask.
<b>any</b>	Displays information for any host.
<b>host hostname</b>	Displays information for a hostname.
<b>host host-ip</b>	Displays information for an IP address.
<i>dst-addr dst-mask</i>	Destination address and mask.
<b>vlan vlan-id</b>	(Optional) Displays information for a specific VLAN; valid values are from 1 to 4094.
<b>statistics</b>	Displays packet and message counts and other statistics.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This command shows how to display the configured VACL-logging properties:

```
Router# show vlan access-log config
VACL Logging Configuration:
    max log table size      :500
    log threshold           :4000
    rate limiter            :3000
Router#
```

This example shows how to display the VACL statistics:

```
Router# show vlan access-log statistics
VACL Logging Statistics:
    total packets      :0
    logged             :0
    dropped            :0
Dropped Packets Statistics:
    unsupported protocol :0
    no packet buffer    :0
    hash queue full     :0
    flow table full     :0
Misc Information:
    VACL Logging LTL Index :0x7E05
    free packet buffers    :8495
    log messages sent     :0
    log table size        :0
Router#
```

---

**Related Commands**

Command	Description
<a href="#">vlan access-log</a>	Configures the VACL-logging properties, including the log-table size, redirect-packet rate, and logging threshold.

---

# 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]
```

<b>Syntax Description</b>	<i>map-name</i> (Optional) VLAN access-map name.
---------------------------	--

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Examples** This command shows how to display the contents of a VLAN-access map:

```
Router# show vlan access-map mordred
Vlan access-map "mordred" 4
    match: ip address 43
    action: forward capture
Router#
show vlan counters
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">action</a>	Sets the packet action clause.
	<a href="#">match</a>	Specifies the match clause by selecting one or more ACLs for a VLAN access-map sequence.
	<a href="#">vlan access-map</a>	Creates a VLAN access map or enters VLAN access-map command mode.

# show vlan counters

To display the software-cached counter values, use the **show vlan counters** command.

**show vlan [id *vlanid*] counters**

<b>Syntax Description</b>	<b>id <i>vlanid</i></b> (Optional) Displays the software-cached counter values for a specific VLAN; valid values are from 1 to 4094.
---------------------------	--

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	<p>The <b>show vlan id counters</b> command is not supported on SVIs.</p> <p>For Layer 2 and Layer 3 VLAN interfaces and router ports, per-interface switching statistics and VLAN-counter information to the PISA are exported approximately every 3 minutes.</p> <p>If you enter the <b>show vlan counters</b> command with no arguments, the software-cached counter values for all VLANs are displayed.</p>
-------------------------	---

<b>Examples</b>	This example shows how to display the software-cached counter values for a specific VLAN:
-----------------	---

```
Router> show vlan id 205 counters
VLAN vlanid 505
L5-Unicast-Pkts      40
L3-In-Unicast-Pkts   0
L3-Out-Unicast-Pkts  0
L5-NonUnicast-Pkts + L3-In-NonUnicast-Pkts  5
L3-Out-NonUnicast-Pkts  6
L5-Unicast-Octets    6
L3-In-Unicast-Octets  6
L3-Out-Unicast-Octets 6
L5-NonUnicast-Octets + L3-In-NonUnicast-Octets 6
L3-Out-NonUnicast-Octets 6
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">clear vlan counters</a>	Clears the software-cached counter values to zero for a specified VLAN or all existing VLANs.

# show vlan dot1q tag native

To display native VLAN-tagging information, use the **show vlan dot1q tag native** command.

**show vlan dot1q tag native**

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

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display native VLAN-tagging information:

```
Router# show vlan dot1q tag native
dot4q native vlan tagging is enabled
Internal dot4q native vlan: 4045
```

```
Router#
```

Related Commands	Command	Description
	<a href="#">vlan dot1q tag native</a>	Enables 802.1Q tagging for all VLANs in a trunk.

# show vlan filter

To display information about the VLAN filter, use the **show vlan filter** command.

```
show vlan filter [{access-map map-name} | {vlan vlan-id} | {interface interface
interface-number}]
```

Syntax Description	
<b>access-map</b> <i>map-name</i>	(Optional) Displays the VLANs that are filtered by the specified map.
<b>vlan</b> <i>vlan-id</i>	(Optional) Displays the filter for the specified VLAN; valid values are from 1 to 4094.
<b>interface</b> <i>interface</i>	Specifies the interface type; valid values are <b>pos</b> , <b>atm</b> , or <b>serial</b> . See the “Usage Guidelines” section for additional information.
<i>interface-number</i>	Interface number; see the “Usage Guidelines” section for additional information.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **show vlan filter** *map-name* **interface** command accepts only ATM, POS, or serial interface types. If your system is not configured with any of these interface types, the **interface** *interface* *interface-number* keyword and arguments are not provided.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 2 to 13 and valid values for the port number are from 1 to 48.

If you do not specify an optional keyword and argument, all mappings are displayed. If you enter **access-map** *map\_name*, all the VLANs and interfaces that are associated with the specified map are shown. If you enter **vlan** *vlan-id* or **interface** *interface* *interface-number*, its associated access map, if existing, is shown.

In the output for VACLs on VLANs, the following applies:

- Configured on VLANs—User configured
- Active on VLANs—VLAN list on which the VACL is active

---

**Examples**

This example shows how to display mappings between the VACLs and the VLANs and the VACLs and the interfaces:

```
Router# show vlan filter
VLAN Map mordred:
  Configured on VLANs: 5,4-6
  Active on VLANs: 5,4-6
Router#
```

---

**Related Commands**

Command	Description
<a href="#">vlan access-map</a>	Creates a VLAN access map or enters VLAN access-map command mode.
<a href="#">vlan filter</a>	Applies a VLAN access map.

# 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**

<b>Syntax Description</b>	<b>id <i>vlan-id</i></b> (Optional) Displays information about the internal VLAN allocation for the specified VLAN; valid values are from 1 to 4094.
---------------------------	--

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

**Command Modes** Privileged EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** In some cases, the output displays the following:

```
workaround vlan
```

A workaround VLAN is used to enable the PFC-based policing on the PWAN1 main interface. Without the workaround VLAN, the packets hit the PFC policer twice for PWAN1 because the same VLAN is used when packets traverse the local bus before and after PXF processing.

**Usage Guidelines** Entering the **show vlan internal usage** command displays the Ethernet interfaces.

**Examples** This example shows how to display the current internal VLAN allocation:

```
Router# show vlan internal usage
```

```
VLAN Usage
-----
4055 -
4056 -
4057 -
4058 -
4059 Port-channel6
4030 GigabitEthernet4/5
4035 FastEthernet3/50
4033 FastEthernet3/54
4459 -
```

This example shows how to display the internal VLAN allocation for a specific VLAN:

```
Router# show vlan id 1030 internal usage
```

```
VLAN Usage  
-----  
4030 GigabitEthernet4/5
```

# show vlan mapping

To register a mapping of an 802.1Q VLAN to an ISL VLAN, use the **show vlan mapping** command.

## show vlan mapping

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

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to list the map for an 802.1Q VLAN to an ISL VLAN:

```
Router# show vlan mapping
80514Q Trunk Remapped VLANs:
80514Q VLAN ISL VLAN
-----
404          505
500          330
Router#
```

Related Commands	Command	Description
	<a href="#">show interfaces vlan mapping</a>	Displays the status of a VLAN mapping on a port.
	<a href="#">switchport vlan mapping enable</a>	Enables VLAN mapping per switch port.

# show vlan private-vlan

To display PVLAN information, use the **show vlan private-vlan** command.

**show vlan private-vlan [type]**

<b>Syntax Description</b>	<b>type</b> (Optional) Displays the PVLAN type (isolated, community, or primary).
---------------------------	---

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

**Command Modes** EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** In the **show vlan private-vlan type** command output display, “normal” displayed as a type indicates a regular VLAN that is configured in a PVLAN. A display of “normal” means that two VLANs have been associated before the type was set and that the PVLAN is not operational. This information is useful for debugging purposes.

**Examples** This example shows how to display information about all currently configured PVLANs:

```
Router# show vlan private-vlan
```

```

Primary Secondary Type          Ports
-----
5         304      community    Fa5/3, Fa5/55
5         305      community
          40       community
400      404      isolated
450      454      non-operational
          505      community
          303      community
404      405      non-operational
Router#
```

This example shows how to display information about all currently configured PVLAN types:

```
Router# show vlan private-vlan type
```

```

Vlan Type
-----
505 primary
303 community
304 community
305 community
306 community
307 community
```

## ■ show vlan private-vlan

```

308 normal
309 community
440 isolated
Router#

```

Table 2-90 describes the fields that are shown in the example.

**Table 2-90** *show vlan private-vlan Command Output Fields*

Field	Description
Primary	Number of the primary VLAN.
Secondary	Number of the secondary VLAN.
Secondary-Type	Secondary VLAN type—Possible values are isolated or community.
Ports	Indicates the ports within a VLAN.
Type	Type of VLAN—Possible values are primary, isolated, community, nonoperation, or normal.

---

**Related Commands**

Command	Description
<a href="#">private-vlan mapping</a>	Creates a mapping between the primary and the secondary VLANs so that both VLANs share the same primary VLAN SVI.
<a href="#">private-vlan</a>	Configures PVLANS and the association between a PVLAN and a secondary VLAN.

# show vlan remote-span

To display a list of 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** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to display a list of remote SPAN VLANs:

```
Router# show vlan remote-span
Remote SPAN VLANs
-----
5, 50
```

Related Commands	Command	Description
	<a href="#">remote-span</a>	Configures a VLAN as an RSPAN VLAN.
	<a href="#">vlan (config-VLAN submode)</a>	Configures a specific VLAN.

# show vlans

To display information about the Cisco IOS VLAN subinterfaces, use the **show vlans** command.

**show vlans** [*vlan*]

<b>Syntax Description</b>	<i>vlan</i> (Optional) VLAN ID number; valid values are from 1 to 4094.
---------------------------	---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	The EXEC <b>show vlan</b> command displays information about the Layer 2 VLAN. The privileged EXEC <b>show vlans</b> command displays information about the VLAN subinterface in Layer 3.
-------------------------	---

When entering the **show vlans** command, you cannot shorten the **vlans** keyword.

<b>Examples</b>	This example shows how to display information about the Cisco IOS VLAN subinterfaces:
-----------------	---

```
Router# show vlans
Virtual LAN ID: 455 (Inter Switch Link Encapsulation)
VLAN Trunk Interface: GE-WAN9/414
Protocols Configured: Address: Received: Transmitted:
IP 4014551015 48 46
Virtual LAN ID: 453 (Inter Switch Link Encapsulation)
VLAN Trunk Interface: GE-WAN9/415
Protocols Configured: Address: Received: Transmitted:
IP 4014531015 43 46
Virtual LAN ID: 454 (Inter Switch Link Encapsulation)
VLAN Trunk Interface: GE-WAN9/413
Protocols Configured: Address: Received: Transmitted:
IP 4014541015 0 47
Virtual LAN ID: 433 (Inter Switch Link Encapsulation)
VLAN Trunk Interface: GE-WAN9/314
Protocols Configured: Address: Received: Transmitted:
IP 4414331014 0 4
Virtual LAN ID: 434 (Inter Switch Link Encapsulation)
VLAN Trunk Interface: GE-WAN9/315
Protocols Configured: Address: Received: Transmitted:
IP 4414341014 0 4
Router#
```

Table 2-91 describes the fields that are shown in the example.

**Table 2-91** *show vlans Command Output Fields*

Field	Description
Virtual LAN ID	Domain number of the VLAN.
VLAN Trunk Interface	Subinterface carrying the VLAN traffic.
Protocols Configured	Protocols that are configured on the VLAN.
Address	Network address.
Received	Number of packets that are received.
Transmitted	Number of packets that are transmitted.

# show vlan virtual-port

To display the number of logical virtual ports required, use the **show vlan virtual-port** command.

**show vlan virtual-port** [*slot num*]

Syntax Description	<i>slot num</i> (Optional) Specifies the slot number of which status is to be displayed.
--------------------	--

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

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Examples	This example shows how to display the number of logical virtual ports that are required for a specific slot:
----------	--

```
Router# show vlan virtual-port slot 3
Slot 3
Port          Virtual-ports
-----
Fa3/4         4
Fa3/5         4
Fa3/3         4
Fa3/4         4
Fa3/5         4
Fa3/6         4
Fa3/7         4
Fa3/8         4
Fa3/44        4
Fa3/45        4
Fa3/43        4
1
1
1
Fa3/33        4
Fa3/34        4
Fa3/35        4
Fa3/36        4
Fa3/37        4
Fa3/38        4
Fa3/39        4
Fa3/40        4
Total virtual ports:85
Router#
```

This example shows how to display the number of logical virtual ports that are required for all slots:

```
Router# show vlan virtual-port
Slot 4
-----
Total slot virtual ports 4
Slot 3
-----
Total slot virtual ports 85
Slot 4
-----
Total slot virtual ports 4
Total chassis virtual ports 87
Router#
```

# show vtp

To display the VTP statistics and domain information, use the **show vtp** command.

```
show vtp {counters | status}
```

Syntax Description	counters	Displays information about the VTP statistics.
	status	Displays information about the VTP domain status.

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

**Command Modes** EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** In the output of the **show vtp status** command, the last modified time is of the modifier itself, for example, the time displayed in the line “Configuration last modified by 7.0.22.11 at 5-5-06 05:51:49”, is the time that the modifier (7.0.22.11) last modified the VLAN configuration.

**Examples** This example shows how to display the VTP statistics:

```
Router# show vtp counters
VTP statistics:
Summary advertisements received      : 4
Subset advertisements received      : 4
Request advertisements received     : 0
Summary advertisements transmitted  : 34
Subset advertisements transmitted   : 4
Request advertisements transmitted   : 0
Number of config revision errors    : 0
Number of config digest errors      : 0
Number of V4 summary errors         : 0

VTP pruning statistics:

Trunk          Join Transmitted Join Received  Summary advts received from
-----          -----          -----          non-pruning-capable device
Pa5/9          4555          4564          0
Router#
```

This example shows how to display the status of the VTP domain:

```
Router# show vtp status
VTP Version          : 5
Configuration Revision : 550
Maximum VLANs supported locally : 4005
```

```

Number of existing VLANs      : 33
VTP Operating Mode           : Server
VTP Domain Name              : Lab_Network
VTP Pruning Mode             : Enabled
VTP V5 Mode                  : Enabled
VTP Traps Generation         : Disabled
MD5 digest                   : 0xE6 0xF8 0x3E 0xDD 0xA4 0xF5 0xC5 0x0E
Configuration last modified by 475150155148 at 9-55-99 44:48:50
Local updater ID is 475150155148 on interface V14 (lowest numbered VLAN interface found)
Router#

```

This example shows how to display only those lines in the **show vtp** output that contain the word **Summary**:

```

Router# show vtp counters | include Summary
Summary advertisements received      : 4
Summary advertisements transmitted : 35
Trunk          Join Transmitted Join Received      Summary advts received from
Router#

```

Table 2-92 describes the fields that are shown in the example.

**Table 2-92 show vtp Command Output Fields**

Field	Description
Summary advts received	Total number of summary advts that are received.
Subset advts received	Total number of subset advts that are received.
Request advts received	Total number of request advts that are received.
Summary advts transmitted	Total number of summary advts that are transmitted.
Subset advts transmitted	Total number of subset advts that are transmitted.
Request advts transmitted	Total number of request advts that are transmitted.
No of config revision errors	Number of config revision errors.
No of config digest errors	Number of config revision digest errors.
Trunk	Trunk port participating in VTP pruning.
Join Transmitted	Number of VTP-Pruning Joins that are transmitted.
Join Received	Number of VTP-Pruning Joins that are received.
Summary advts received from non-pruning-capable device	Number of Summary advts that are received from nonpruning-capable devices.
Number of existing VLANs	Total number of VLANs in the domain.
Configuration Revision	VTP revision number that is used to exchange VLAN information.
Maximum VLANs supported locally	Maximum number of VLANs that are allowed on the device.
Number of existing VLANs	Number of existing VLANs.
VTP Operating Mode	Status on whether VTP is enabled or disabled.

*Table 2-92 show vtp Command Output Fields (continued)*

Field	Description
VTP Domain Name	Name of the VTP domain.
VTP Pruning Mode	Status on whether VTP pruning is enabled or disabled.
VTP V2 Mode	Status of the VTP V2 mode as server, client, or transparent.
VTP Traps Generation	Status on whether VTP-trap generation mode is enabled or disabled.
MD5 digest	Checksum values.

**Related Commands**

Command	Description
<a href="#">vtp</a>	Configures the global VTP state.

# shutdown vlan

To shut down local traffic on a specified VLAN, use the **shutdown vlan** command. To restart local traffic on the VLAN, use the **no** form of this command.

**shutdown vlan** *vlan-id*

**no shutdown vlan** *vlan-id*

<b>Syntax Description</b>	<i>vlan-id</i>	VLAN number of the VLAN to be locally shut down; valid values are from 2 to 1001.
---------------------------	----------------	---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	This command does not support extended-range VLANs.
-------------------------	---

<b>Examples</b>	This example shows how to shut down traffic on VLAN 2:
-----------------	--

```
Router(config)# shutdown vlan 2
Router(config)#
```

# snmp ifindex clear

To clear any previously configured **snmp ifindex** commands that were issued 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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**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.

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 that were previously entered for that specific interface.

When you clear the ifIndex configuration, the ifIndex persistence is enabled for all interfaces as specified by the **snmp-server ifindex persist** command in global configuration mode.

**Examples** This example shows how to enable ifIndex persistence for all interfaces:

```
Router(config)# snmp ifindex persist
```

This example shows how to disable IfIndex persistence for Ethernet 0/1 only:

```
Router(config)# interface ethernet 0/1
Router(config-if)# no snmp ifindex persist
Router(config-if)# exit
```

This example shows how to clear the ifIndex configuration from the Ethernet 0/1 configuration:

```
Router(config)# interface ethernet 0/1
Router(config-if)# snmp ifindex clear
Router(config-if)# exit
```

Related Commands	Command	Description
	<a href="#">snmp ifindex persist</a>	Enables ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) only on a specific interface.
	<a href="#">snmp-server ifindex persist</a>	Enables ifIndex values globally so that they 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) only 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

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**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** command in interface configuration mode 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** command in global configuration mode 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.

IfIndex commands that you configure for an interface apply to all subinterfaces on that interface.

**Examples** This example shows how to enable ifIndex persistence for interface Ethernet 0/1 only:

```
Router(config)# interface ethernet 0/1
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 Ethernet 0/1 only:

```
Router(config)# snmp ifindex persist
Router(config)# interface ethernet 0/1
Router(config-if)# no snmp ifindex persist
Router(config-if)# exit
```

---

**Related Commands**

Command	Description
<a href="#">snmp ifindex clear</a>	Clears any previously configured <b>snmp ifindex</b> commands that were issued for a specific interface.
<a href="#">snmp-server ifindex persist</a>	Enables ifIndex values globally so that they remain constant across reboots for use by SNMP.

## snmp-server enable traps

To enable the SNMP notifications (traps or informs) that are available on your system, use the **snmp-server enable traps** command. To disable all available SNMP notifications, use the **no** form of this command.

**snmp-server enable traps** [*notification-type*]

**no snmp-server enable traps** [*notification-type*]

<b>Syntax Description</b>	<i>notification-type</i>	(Optional) Type of notification (trap or inform) to enable or disable. If no type is specified, all notifications that are available on your device are enabled or disabled. See the “Usage Guidelines” section for valid values.
---------------------------	--------------------------	---

<b>Defaults</b>	<p>This command is disabled by default. Most notification types are disabled. However, some notification types cannot be controlled with this command.</p> <p>If you enter this command without a <i>notification-type</i>, all notification types that are controlled by this command are enabled.</p>
-----------------	---

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

<b>Command History</b>	<table border="1"> <thead> <tr> <th style="border: none;">Release</th> <th style="border: none;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border: none;">12.2(18)ZY</td> <td style="border: none;">Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)ZY	Support for this command was introduced.
Release	Modification				
12.2(18)ZY	Support for this command was introduced.				

<b>Usage Guidelines</b>	<p>For additional notification types, refer to the <i>Cisco IOS Release 12.2 Command Reference</i>.</p> <p>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 <b>snmp-server host</b> [<b>traps</b>   <b>informs</b>] command.</p> <p>If you do not enter an <b>snmp-server enable traps</b> command, no notifications that are controlled by this command are sent. To configure the router to send these SNMP notifications, you must enter at least one <b>snmp-server enable traps</b> command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type that is related to that keyword is enabled. To enable multiple types of notifications, you must issue a separate <b>snmp-server enable traps</b> command for each notification type and notification option.</p> <p>The <b>snmp-server enable traps</b> command is used with the <b>snmp-server host</b> command. Use the <b>snmp-server host</b> command to specify which host or hosts receive SNMP notifications. To send notifications, you must configure at least one <b>snmp-server host</b> command.</p> <p>The following list of MIBs are used for the traps:</p> <ul style="list-style-type: none"> <li>• <b>chassis</b>—Controls the chassisAlarm traps from the CISCO-STACK-MIB</li> <li>• <b>flash</b>—Controls SNMP flash traps from the CISCO-FLASH-MIB             <ul style="list-style-type: none"> <li>– <b>insertion</b>—Controls the SNMP flash insertion-trap notifications</li> </ul> </li> </ul>
-------------------------	---

- **removal**—Controls the SNMP flash removal-trap notifications
- **fru-ctrl**—Controls the FRU-control traps from the CISCO-ENTITY-FRU-CONTROL-MIB
- **module**—Controls the SNMP-module traps from the CISCO-STACK-MIB
- **stp**—Controls all the traps from the CISCO-STP-EXTENSIONS-MIB
- **vlancreate**—Controls the SNMP VLAN-created trap notifications
- **vlandelete**—Controls the SNMP VLAN-deleted trap notifications
- **vtp**—Controls the VTP traps from the CISCO-VTP-MIB

The following SNMP-server enable traps are supported:

- **bridge**—Controls the STP Bridge MIB traps
- **c6kxbar**—Controls the c6kxbar intbus-crcexcd intbus-crcrcvrd swbus trap
- **csg**—Controls the CSG agent quota database traps
- **flex-links**—Controls the flex-links status traps
- **mac-notification**—Controls the MAC-Notification move threshold traps
- **stp**—Controls the STPX inconsistency root-inconsistency loop-inconsistency traps
- **vlan-mac-limit**—Controls the Layer 2 control VLAN MAC limit notifications traps

---

### Examples

This example shows how to send all traps to the host that are specified by the name myhost.cisco.com, using the community string that is defined as public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com public
```

# snmp-server enable traps transceiver type all

To enable all supported SNMP transceiver traps for all transceiver types, use the **snmp-server enable traps transceiver type all** command. To disable the transceiver SNMP trap notifications, use the **no** form of this command.

**snmp-server enable traps transceiver type all**

**no snmp-server enable traps transceiver type all**

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

**Defaults** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **snmp-server enable traps** command is used 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.

**Examples** This example shows how to enable all supported SNMP transceiver traps for all transceiver types:

```
Router(config)# snmp-server enable traps transceiver type all
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show interfaces transceiver</a>	Displays information about the optical transceivers that have DOM enabled.

# snmp-server ifindex persist

To enable ifIndex values globally so that they will remain constant across reboots for use by SNMP, use the **snmp-server ifindex persist** command. To disable ifIndex persistence globally, 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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**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** command in global configuration mode does not override interface-specific configurations. To override the interface-specific configuration of ifIndex persistence, enter the **[no] snmp ifindex persist** and **snmp ifindex clear** commands in interface configuration mode.

Entering the **[no] snmp-server ifindex persist** command in global configuration mode 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
Router(config)#
```

**Note**

This example shows that if ifIndex persistence was previously disabled for a specific interface using the **no snmp ifindex persist** command in interface configuration mode, ifIndex persistence remains disabled for that interface. The global ifIndex command does not override the interface-specific commands.

**Related Commands**

Command	Description
<a href="#">snmp ifindex clear</a>	Clears any previously configured <b>snmp ifindex</b> commands that were issued for a specific interface.
<a href="#">snmp ifindex persist</a>	Enables ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) only on a specific interface.

# snmp-server source-interface

To specify the interface from which a SNMP trap originates the informs or traps, use the **snmp-server source-interface** command. To remove the source designation, use the **no** form of the command.

```
snmp-server source-interface {traps | informs} interface
```

```
no snmp-server source-interface {traps | informs} [interface]
```

## Syntax Description

<b>traps</b>	Specifies SNMP traps.
<b>informs</b>	Specifies SNMP informs.
<i>interface</i>	Specifies the interface type and the module and port number of the source interface.

## Defaults

No interface is designated.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

The source interface must have an IP address.

Enter the *interface* argument in the following format: *interface-type/module/port*.

An SNMP trap or inform sent from a Cisco SNMP server has a notification IP address of the interface it went out of at that time. Use this command to monitor notifications from a particular interface.

## Examples

This example shows how to specify that the interface gigabitethernet5/2 is the source for all informs:

```
Router(config)# snmp-server source-interface informs gigabitethernet5/2
Router(config)#
```

This example shows how to specify that the interface gigabitethernet5/3 is the source for all traps:

```
Router(config)# snmp-server source-interface traps gigabitethernet5/3
Router(config)#
```

This example shows how to remove the source designation for all traps for a specific interface:

```
Router(config)# no snmp-server source-interface traps gigabitethernet5/3
Router(config)#
```

## Related Commands

Command	Description
<b>snmp-server trap-source interface</b>	Specifies the interface from which a SNMP trap should originate. This command has been replaced by the <b>snmp-server source-interface</b> command.
<b>snmp-server enable traps</b>	Enables a router to send SNMP traps and informs.
<b>snmp-server host</b>	Specifies the recipient of a SNMP notification operation.

# snmp-server trap authentication unknown-context

To enable the authorization failure traps during an unknown context error, use the **snmp-server trap authentication unknown-context** command. To disable the the authorization failure traps, use the **no** form of this command.

**snmp-server trap authentication unknown-context**

**no snmp-server trap authentication unknown-context**

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

**Defaults** No authFail traps are generated.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to enable the authorization failure traps during an unknown context error:

```
Router(config)# snmp-server trap authentication unknown-context
Router(config)#
```

This example shows how to disable the authorization failure traps during an unknown context error:

```
Router(config)# no snmp-server trap authentication unknown-context
Router(config)#
```

## snmp-server trap link switchover

To enable sending a linkdown trap followed by a linkup trap for every interface in the switch during a switch failover, use the **snmp-server trap link switchover** command. To disable linkdown during a switch failover, use the **no** form of this command.

**snmp-server trap link switchover**

**no snmp-server trap link switchover**

---

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

---

**Defaults** Enabled

---

**Command Modes** Global configuration

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Usage Guidelines** By default, no link traps are generated during a switchover.

---

**Examples** This example shows how to return to the default setting:

```
Router(config)# snmp-server trap link switchover
Router(config)#
```

This example shows how to disable linkdown followed by a linkup trap for every interface in the switch during a switch failover:

```
Router(config)# no snmp-server trap link switchover
Router(config)#
```

# spanning-tree backbonefast

To enable BackboneFast on all Ethernet VLANs, 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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Enable BackboneFast on all Catalyst 6500 series switches to allow the detection of indirect link failures to start spanning-tree reconfiguration sooner.

**Examples** This example shows how to enable BackboneFast on all Ethernet VLANs:

```
Router(config)# spanning-tree backbonefast
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show spanning-tree</a>	Displays information about the spanning-tree state.

# spanning-tree bpdudfilter

To enable BPDU filtering on the interface, use the **spanning-tree bpdudfilter** command. To return to the default settings, use the **no** form of this command.

**spanning-tree bpdudfilter** { **enable** | **disable** }

**no spanning-tree bpdudfilter**

Syntax Description	enable	Enables BPDU filtering on this interface.
	<b>disable</b>	Disables BPDU filtering on this interface.

**Defaults** The setting that is already configured when you enter the **spanning-tree portfast bpdudfilter default** command.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines



Caution

Be careful when you enter the **spanning-tree bpdudfilter enable** command. Enabling BPDU filtering on an interface is similar to disabling the spanning tree for this interface. If you do not use this command correctly, you might create bridging loops.

Entering the **spanning-tree bpdudfilter enable** command to enable BPDU filtering overrides the PortFast configuration.

When configuring Layer 2-protocol tunneling on all the service-provider edge switches, you must enable spanning-tree BPDU filtering on the 802.1Q tunnel ports by entering the **spanning-tree bpdudfilter enable** command.

BPDU filtering prevents a port from sending and receiving BPDUs. The configuration is applicable to the whole interface, whether it is trunking or not. This command has three states:

- **spanning-tree bpdudfilter enable**—Unconditionally enables BPDU filtering on the interface.
- **spanning-tree bpdudfilter disable**—Unconditionally disables BPDU filtering on the interface.
- **no spanning-tree bpdudfilter**—Enables BPDU filtering on the interface if the interface is in operational PortFast state and if you configure the **spanning-tree portfast bpdudfilter default** command.

Use the **spanning-tree portfast bpdudfilter default** command to enable BPDU filtering on all ports that are already configured for PortFast.

---

**Examples**

This example shows how to enable BPDU filtering on this interface:

```
Router(config-if)# spanning-tree bpdudfilter enable  
Router(config-if)#
```

---

**Related Commands**

Command	Description
<a href="#">show spanning-tree</a>	Displays information about the spanning-tree state.
<a href="#">spanning-tree portfast bpdudfilter default</a>	Enables BPDU filtering by default on all PortFast ports.

## spanning-tree bpduguard

To enable BPDU guard on the 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** The setting that is already configured when you enter the **spanning-tree portfast bpduguard default** command.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** BPDU guard prevents a port from receiving BPDUs. Typically, this feature is used in a service-provider environment where the network 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 error-disabled state as a protective measure. This command has three states:

- **spanning-tree bpduguard enable**—Unconditionally enables BPDU guard on the interface.
- **spanning-tree bpduguard disable**—Unconditionally disables BPDU guard on the interface.
- **no spanning-tree bpduguard**—Enables BPDU guard on the interface if 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:

```
Router(config-if)# spanning-tree bpduguard enable
Router(config-if)#
```

Related Commands	Command	Description
	<b>show spanning-tree</b>	Displays information about the spanning-tree state.
	<b>spanning-tree portfast bpduguard default</b>	Enables BPDU guard by default on all PortFast ports.

# spanning-tree cost

To set the path cost of the interface for STP calculations, use the **spanning-tree cost** command. To return to the default settings, use the **no** form of this command.

**spanning-tree cost** *cost*

**no spanning-tree cost**

## Syntax Description

<i>cost</i>	Path cost; valid values are from 1 to 200000000.
-------------	--

## Defaults

The default path cost is computed from the interface's bandwidth setting; the default path costs are as follows:

- Ethernet—100
- 16-Mb Token Ring—62
- FDDI—10
- FastEthernet—10
- ATM 155—6
- GigabitEthernet—1
- 10-Gigabit Ethernet—2
- HSSI—647

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

When you configure the *cost*, note that higher values indicate higher costs. This range applies regardless of the protocol type that is specified.

## Examples

This example shows how to access an interface and set a path cost value of 250 for the spanning-tree VLAN that is associated with that interface:

```
Router(config)# interface ethernet 2/0
Router(config-if)# spanning-tree cost 250
Router(config-if)#
```

## Related Commands

Command	Description
<a href="#">show spanning-tree</a>	Displays information about the spanning-tree state.

# 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 error message, use the **no** form of this command.

**spanning-tree etherchannel guard misconfig**

**no spanning-tree etherchannel guard misconfig**

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

**Defaults** Enabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** EtherChannel uses either PAgP or LACP and does not work if the EtherChannel mode of the interface has been enabled using the **channel-group group-number mode on** command.

When an EtherChannel-guard misconfiguration is detected, this error message displays:

```
msgdef(CHNL_MISCFG, SPANTREE, LOG_CRIT, 0, "Detected loop due to etherchannel
misconfiguration of %s %s")
```

To determine which local ports are involved in the misconfiguration, enter the **show interfaces status err-disabled** command. To check the EtherChannel configuration on the remote device, enter the **show etherchannel summary** command on the remote device.

After you correct the configuration, enter the **shutdown** and the **no shutdown** commands on the associated port-channel interface.

**Examples** This example shows how to enable the EtherChannel-guard misconfiguration:

```
Router(config)# spanning-tree etherchannel guard misconfig
Router(config)#
```

Related Commands	Command	Description
	<b>show etherchannel summary</b>	Displays the EtherChannel information for a channel.

Command	Description
<b>show interfaces status err-disabled</b>	Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.
<b>shutdown</b>	Disables an interface.

## spanning-tree extend system-id

To enable the extended-system ID feature on chassis that support 1024 MAC addresses, use the **spanning-tree extend system-id** command. To disable the extended system identification, use the **no** form of this command.

**spanning-tree extend system-id**

**no spanning-tree extend system-id**

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

**Defaults** Enabled on systems that do not provide 1024 MAC addresses.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The Catalyst 6500 series switch can support 64 or up to 1024 MAC addresses. For a Catalyst 6500 series switch with 64 MAC addresses, STP uses the extended-system ID and a MAC address to make the bridge ID unique for each VLAN.

You cannot disable the extended-system ID on a Catalyst 6500 series switch that supports 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:

```
Router(config)# spanning-tree extend system-id
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show spanning-tree</a>	Displays information about the spanning-tree state.

# spanning-tree guard

To enable or disable the guard mode, use the **spanning-tree guard** command. To return to the default settings, use the **no** form of this command.

**spanning-tree guard {loop | root | none}**

**no spanning-tree guard**

Syntax Description	Command	Description
	<b>loop</b>	Enables the loop-guard mode on the interface.
	<b>root</b>	Enables root-guard mode on the interface.
	<b>none</b>	Sets the guard mode to none.

**Defaults** Guard mode is disabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to enable root guard:

```
Router(config-if)# spanning-tree guard root
Router(config-if)#
```

Related Commands	Command	Description
	<a href="#">show spanning-tree</a>	Displays information about the spanning-tree state.
	<a href="#">spanning-tree loopguard default</a>	Enables loop guard as a default on all ports of a given bridge.

# 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

<b>point-to-point</b>	Specifies that the interface is a point-to-point link.
<b>shared</b>	Specifies that the interface is a shared medium.

## Defaults

Link type is automatically derived from the duplex setting unless you explicitly configure the link type.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## 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.

If you designate a port as a shared link, RSTP+ fast transition is forbidden, regardless of the duplex setting.

## Examples

This example shows how to configure the port as a shared link:

```
Router(config-if)# spanning-tree link-type shared
Router(config-if)#
```

## Related Commands

Command	Description
<b>show spanning-tree interface</b>	Displays information about the spanning-tree state.

# spanning-tree loopguard default

To enable loop guard as a default on all ports of a given bridge, use the **spanning-tree loopguard default** command. To disable loop guard, use the **no** form of this command.

**spanning-tree loopguard default**

**no spanning-tree loopguard default**

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

**Defaults** Loop guard is disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Loop guard provides additional security in the bridge network. Loop guard prevents alternate or root ports from becoming the designated port due to a failure that could lead to a unidirectional link. Loop guard operates only on ports that are considered point to point by the spanning tree. The individual loop-guard port configuration overrides this command.

**Examples** This example shows how to enable loop guard:

```
Router(config)# spanning-tree loopguard default
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show spanning-tree</a>	Displays information about the spanning-tree state.
	<a href="#">spanning-tree guard</a>	Enables or disables the guard mode.

## spanning-tree mode

To switch between PVST+, Rapid-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**

Syntax Description	
<b>pvst</b>	(Optional) PVST+ mode.
<b>mst</b>	(Optional) MST mode.
<b>rapid-pvst</b>	(Optional) Rapid-PVST+ mode.

Defaults	
<b>pvst</b>	

Command Modes	
Global configuration	

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines



#### Caution

Be careful when using the **spanning-tree mode** command to switch between PVST+, Rapid-PVST+, and MST modes. When you enter the command, all spanning-tree instances are stopped for the previous mode and are restarted in the new mode. Using this command may cause the user traffic to be disrupted.

### Examples

This example shows how to switch to MST mode:

```
Router(config)# spanning-tree mode mst
Router(config)#
```

This example shows how to return to the default mode (PVST+):

```
Router(config)# no spanning-tree mode
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show spanning-tree mst</a>	Displays the information about the MST protocol.

## 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}
```

### Syntax Description

<i>instance-id</i>	Instance ID number; valid values are from 0 to 15.
<b>cost</b> <i>cost</i>	(Optional) Path cost for an instance; valid values are from 1 to 200000000.
<b>port-priority</b> <i>prio</i>	(Optional) Port priority for an instance; valid values are from 0 to 240 in increments of 16.

### Defaults

The defaults are as follows:

- *cost* depends on the port speed; the faster interface speeds indicate smaller costs. MST always uses long path costs.
- *prio* is **128**.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

Higher **cost** *cost* values indicate higher costs. When entering the *cost*, do not include a comma in the entry; for example, enter **1000**, not **1,000**.

Higher **port-priority** *prio* values indicate smaller priorities.

### Examples

This example shows how to set the interface path cost:

```
Router(config-if)# spanning-tree mst 0 cost 17031970
Router(config-if)#
```

This example shows how to set the interface priority:

```
Router(config-if)# spanning-tree mst 0 port-priority 64
Router(config-if)#
```

## ■ spanning-tree mst

Related Commands	Command	Description
	<a href="#">show spanning-tree mst</a>	Displays the information about the MST protocol.
	<a href="#">spanning-tree port-priority</a>	Sets an interface priority when two bridges vie for position as the root bridge.

# spanning-tree mst configuration

To enter MST-configuration submode, use the **spanning-tree mst configuration** command. To return to the default settings, use the **no** form of this command.

**spanning-tree mst configuration**

**no spanning-tree mst configuration**

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

**Defaults** The default value for the MST configuration is the default value for all its parameters:

- No VLANs are mapped to any MST instance (all VLANs are mapped to the CIST instance).
- The region name is an empty string.
- The revision number is 0.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The MST configuration consists of three main parameters:

- Instance VLAN mapping—See the **instance** command
- Region name—See the **name (MST configuration submode)** command
- Configuration revision number—See the **revision** command

The **abort** and **exit** commands allow you to exit MST configuration submode. The difference between the two commands depends on whether you want to save your changes or not.

The **exit** command commits all the changes before leaving MST configuration submode. If you do not map secondary VLANs to the same instance as the associated primary VLAN, when you exit MST-configuration submode, a warning message displays and lists the secondary VLANs that are not mapped to the same instance as the associated primary VLAN. The warning message is as follows:

```
These secondary vlans are not mapped to the same instance as their primary:
-> 3
```

The **abort** command leaves MST-configuration submode without committing any changes.

Changing an MST-configuration submode parameter can cause connectivity loss. To reduce service disruptions, when you enter MST-configuration submode, make changes to 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 commit a new configuration at exactly at the same time, this warning message displays:

```
% MST CFG:Configuration change lost because of concurrent access
```

## Examples

This example shows how to enter MST-configuration submode:

```
Router(config)# spanning-tree mst configuration
Router(config-mst)#
```

This example shows how to reset the MST configuration to the default settings:

```
Router(config)# no spanning-tree mst configuration
Router(config)#
```

## Related Commands

Command	Description
<a href="#">instance</a>	Maps a VLAN or a set of VLANs to an MST instance.
<a href="#">name (MST configuration submode)</a>	Sets the name of an MST region.
<a href="#">revision</a>	Sets the revision number for the MST configuration.
<a href="#">show</a>	Verifies the MST configuration.
<a href="#">show spanning-tree mst</a>	Displays the information about the MST protocol.

## spanning-tree mst forward-time

To set the forward-delay timer for all the instances on the Catalyst 6500 series switch, 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**

<b>Syntax Description</b>	<i>seconds</i>	Number of seconds to set the forward-delay timer for all the instances on the Catalyst 6500 series switch; valid values are from 4 to 30 seconds.
<b>Defaults</b>	<i>seconds</i> is <b>15</b> .	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.
<b>Examples</b>	<p>This example shows how to set the forward-delay timer:</p> <pre>Router(config)# spanning-tree mst forward-time 20 Router(config)#</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show spanning-tree mst</a>	Displays the information about the MST protocol.

## spanning-tree mst hello-time

To set the hello-time delay timer for all the instances on the Catalyst 6500 series switch, 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**

<b>Syntax Description</b>	<i>seconds</i>	Number of seconds to set the hello-time delay timer for all the instances on the Catalyst 6500 series switch; valid values are from 1 to 10 seconds.
---------------------------	----------------	--

<b>Defaults</b>	2 seconds
-----------------	-----------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	If you do not specify the <i>hello-time</i> value, the value is calculated from the network diameter.
-------------------------	---

<b>Examples</b>	This example shows how to set the hello-time delay timer:
-----------------	---

```
Router(config)# spanning-tree mst hello-time 3
Router(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show spanning-tree mst</a>	Displays the information about the MST protocol.

# spanning-tree mst max-age

To set the max-age timer for all the instances on the Catalyst 6500 series switch, 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**

<b>Syntax Description</b>	<i>seconds</i>	Number of seconds to set the max-age timer for all the instances on the Catalyst 6500 series switch; valid values are from 6 to 40 seconds.				
<b>Defaults</b>	20 seconds					
<b>Command Modes</b>	Global configuration					
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(18)ZY</td> <td>Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)ZY	Support for this command was introduced.	
Release	Modification					
12.2(18)ZY	Support for this command was introduced.					
<b>Examples</b>	<p>This example shows how to set the max-age timer:</p> <pre>Router(config)# spanning-tree mst max-age 40 Router(config)#</pre>					
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><a href="#">show spanning-tree mst</a></td> <td>Displays the information about the MST protocol.</td> </tr> </tbody> </table>	Command	Description	<a href="#">show spanning-tree mst</a>	Displays the information about the MST protocol.	
Command	Description					
<a href="#">show spanning-tree mst</a>	Displays the information about the MST protocol.					

## 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**

<b>Syntax Description</b>	<i>hopnumber</i>	Number of possible hops in the region before a BPDU is discarded; valid values are from 1 to 255 hops.
---------------------------	------------------	--

<b>Defaults</b>	20 hops
-----------------	---------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Examples** This example shows how to set the number of possible hops:

```
Router(config)# spanning-tree mst max-hops 25
Router(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show spanning-tree mst</a>	Displays the information about the MST protocol.

# spanning-tree mst pre-standard

To configure a port to transmit only prestandard BPDUs, use the **spanning-tree mst pre-standard** command. To return to the default settings, use the **no** form of this command.

**spanning-tree mst pre-standard**

**no spanning-tree mst pre-standard**

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

**Defaults** The default is to automatically detect prestandard neighbors.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Even with the default configuration, the port can receive both prestandard and standard BPDUs. Prestandard BPDUs are based on the Cisco IOS MST implementation that was created before the IEEE standard was finalized. Standard BPDUs are based on the finalized IEEE standard.

If you configure a port to transmit prestandard BPDUs only, the prestandard flag displays in the **show spanning-tree** commands. The variations of the prestandard flag are as follows:

- Pre-STD (or prestandard in long format)—This flag displays if the port is configured to transmit prestandard BPDUs and if a prestandard neighbor bridge has been detected on this interface.
- Pre-STD-Cf (or prestandard (config) in long format)—This flag displays if the port is configured to transmit prestandard BPDUs but a prestandard BPDU has not been received on the port, the autodetection mechanism has failed, or a misconfiguration, if there is no prestandard neighbor, has occurred.
- Pre-STD-Rx (or prestandard (rcvd) in long format)—This flag displays when a prestandard BPDU has been received on the port but it has not been configured to send prestandard BPDUs. The port will send prestandard BPDUs, but we recommend that you change the port configuration so that the interaction with the prestandard neighbor does not rely only on the autodetection mechanism.

If the MST configuration is not compatible with the prestandard (if it includes an instance ID greater than 15), only standard MST BPDUs are transmitted, regardless of the STP configuration on the port.

**Examples** This example shows how to configure a port to transmit only prestandard BPDUs:

```
Router(config-if)# spanning-tree mst pre-standard
Router(config-if)#
```

## ■ spanning-tree mst pre-standard

Related Commands	Command	Description
	<a href="#">show spanning-tree mst</a>	Displays information about the MST protocol.

## spanning-tree mst root

To designate the primary and secondary root, set the bridge priority, and set the 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-time]]
```

```
no spanning-tree mst root
```

Syntax Description	
<i>instance-id</i>	Instance identification number; valid values are from 1 to 15.
<b>primary</b>	Specifies the high enough priority (low value) to make the bridge root of the spanning-tree instance.
<b>secondary</b>	Specifies the switch as a secondary root, should the primary root fail.
<b>priority</b> <i>prio</i>	Specifies the bridge priority; see the “Usage Guidelines” section for valid values and additional information.
<b>diameter</b> <i>dia</i>	(Optional) Specifies the timer values for the bridge that are based on the network diameter; valid values are from 1 to 7.
<b>hello-time</b> <i>hello-time</i>	(Optional) Specifies the duration between the generation of configuration messages by the root switch.

### Defaults

The defaults are as follows:

- **spanning-tree mst root** has no default settings.
- *prio* is **32768**.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

You can set the bridge priority in increments of 4096 only. When you set the priority, valid values are **0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344,** and **61440**.

You can set the *prio* to **0** to make the switch root.

You can enter the *instance-id* as a single instance or a range of instances, for example, 0-3,5,7-9.

The **spanning-tree root secondary** bridge priority value is 16384.

The **diameter** *dia* and **hello-time** *hello-time* keywords and arguments are available for instance 0 only.

If you do not specify the *hello-time* argument, the argument is calculated from the network diameter.

---

**Examples**

This example shows how to set the bridge priority:

```
Router(config)# spanning-tree mst 0 root priority 4096
Router(config)#
```

This example shows how to set the priority and timer values for the bridge:

```
Router(config)# spanning-tree mst 0 root primary diameter 7 hello-time 2
Router(config)# spanning-tree mst 5 root primary
Router(config)#
```

---

**Related Commands**

Command	Description
<a href="#">show spanning-tree mst</a>	Displays the information about the MST protocol.

# spanning-tree pathcost method

To set the default path-cost calculation method, use the **spanning-tree pathcost method** command. To return to the default settings, use the **no** form of this command.

**spanning-tree pathcost method {long | short}**

**no spanning-tree pathcost method**

Syntax Description	long	Specifies the 32-bit based values for default port-path costs.
	short	Specifies the 16-bit based values for default port-path costs.

Defaults	<b>short</b>
----------	--------------

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Usage Guidelines	<p>This command applies to all the spanning-tree instances on the Catalyst 6500 series switch.</p> <p>The <b>long</b> path-cost calculation method utilizes all 32 bits for path-cost calculation and yields values in the range of 1 through 200,000,000.</p> <p>The <b>short</b> path-cost calculation method (16 bits) yields values in the range of 1 through 65535.</p>
------------------	--

Examples	This example shows how to set the default path-cost calculation method to long:
----------	---

```
Router(config)# spanning-tree pathcost method long
Router(config)#
```

This example shows how to set the default path-cost calculation method to short:

```
Router(config)# spanning-tree pathcost method short
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show spanning-tree</a>	Displays information about the spanning-tree state.

## 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 settings, use the **no** form of this command.

**spanning-tree portfast**

**spanning-tree portfast { disable | trunk }**

**no spanning-tree portfast**

Syntax Description	disable	Disables PortFast on the interface.
	<b>trunk</b>	Enables PortFast on the interface even in the trunk mode.

**Defaults** The settings that are configured by the **spanning-tree portfast default** command.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** You should use this command only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data-packet loop and disrupt the Catalyst 6500 series switch and network operation.

An interface with PortFast mode enabled is moved directly to the spanning-tree forwarding state when linkup occurs without waiting for the standard forward-time delay.

Be careful when using the **no spanning-tree portfast** command. This command does not disable PortFast if the **spanning-tree portfast default** command is enabled.

This command has four states:

- **spanning-tree portfast**—This command enables PortFast unconditionally on the given port.
- **spanning-tree portfast disable**—This command explicitly disables PortFast for the given port. The configuration line shows up in the running configuration because it is not the default.
- **spanning-tree portfast trunk**—This command allows you to configure PortFast on trunk ports.



**Note** If you enter the **spanning-tree portfast trunk** command, the port is configured for PortFast even in the access mode.

- **no spanning-tree portfast**—This command implicitly enables PortFast if you define the **spanning-tree portfast default** command in global configuration mode 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:

```
Router(config-if)# spanning-tree portfast
Router(config-if)#
```

---

### Related Commands

Command	Description
<b>show spanning-tree</b>	Displays information about the spanning-tree state.
<b>spanning-tree portfast default</b>	Enables PortFast by default on all access ports.

# spanning-tree portfast bpdudfilter default

To enable BPDU filtering by default on all PortFast ports, use the **spanning-tree portfast bpdudfilter default** command. To return to the default settings, use the **no** form of this command.

**spanning-tree portfast bpdudfilter default**

**no spanning-tree portfast bpdudfilter default**

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

**Defaults** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The **spanning-tree portfast bpdudfilter** command enables BPDU filtering globally on PortFast ports. BPDU filtering prevents a port from sending or receiving any BPDUs.

You can override the effects of the **portfast bpdudfilter default** command by configuring BPDU filtering at the interface level.



**Note**

Be careful when enabling BPDU filtering. The feature's functionality is different when you enable it 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 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 6500 series switch from receiving or sending BPDUs on this port.



**Caution**

Be careful when using this command. Using this command incorrectly can cause bridging loops.

This example shows how to enable BPDU filtering by default:

```
Router(config)# spanning-tree portfast bpdudfilter default
Router(config)#
```

**Related Commands**

Command	Description
<a href="#">show spanning-tree mst</a>	Displays the information about the MST protocol.
<a href="#">spanning-tree bpdudfilter</a>	Enables BPDU filtering on the interface.

# spanning-tree portfast bpduguard default

To enable BPDU guard by default on all PortFast ports, use the **spanning-tree portfast bpduguard default** command. To return to the default settings, use the **no** form of this command.

**spanning-tree portfast bpduguard default**

**no spanning-tree portfast bpduguard default**

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

**Defaults** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines



### Caution

Be careful when using this command. You should use this command only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data-packet loop and disrupt the Catalyst 6500 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:

```
Router(config)# spanning-tree portfast bpduguard default
Router(config)#
```

Related Commands	Command	Description
	<a href="#">show spanning-tree mst</a>	Displays the information about the MST protocol.
	<a href="#">spanning-tree portfast bpduguard default</a>	Enables the BPDU guard on the interface.

# spanning-tree portfast default

To enable PortFast by default on all access ports, use the **spanning-tree portfast default** command. To disable PortFast by default on all access ports, use the **no** form of this command.

**spanning-tree portfast default**

**no spanning-tree portfast default**

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

**Defaults** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines



### Caution

Be careful when using this command. You should use this command only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data-packet loop and disrupt the Catalyst 6500 series switch and network operation.

An interface with PortFast mode enabled is moved directly to the spanning-tree forwarding state when linkup occurs without waiting for the standard forward-time delay.

You can enable PortFast mode on individual interfaces using the **spanning-tree portfast (interface configuration mode)** command.

**Examples** This example shows how to enable PortFast by default on all access ports:

```
Router(config)# spanning-tree portfast default
Router(config)#
```

Related Commands	Command	Description
	<b>show spanning-tree</b>	Displays information about the spanning-tree state.
	<b>spanning-tree portfast (interface configuration mode)</b>	Enables PortFast mode.

## spanning-tree port-priority

To set an interface priority when two bridges vie for position as the root bridge, use the **spanning-tree port-priority** command. The priority you set breaks the tie. To return to the default settings, use the **no** form of this command.

**spanning-tree port-priority** *port-priority*

**no spanning-tree port-priority**

<b>Syntax Description</b>	<i>port-priority</i> Port priority; valid values are from 2 to 255.
---------------------------	---

<b>Defaults</b>	<i>port-priority</i> is <b>128</b> .
-----------------	--------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Examples</b>	This example shows how to increase the likelihood that the spanning-tree instance 20 is chosen as the root bridge on Ethernet interface 2/0:
-----------------	--

```
Router(config-if)# spanning-tree port-priority 0
Router(config-if)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show spanning-tree</a>	Displays information about the spanning-tree state.
	<a href="#">spanning-tree mst</a>	Sets the path cost and port-priority parameters for any MST instance (including the CIST with instance ID 0).
	<a href="#">spanning-tree vlan</a>	Configures STP on a per-VLAN basis.

# spanning-tree transmit hold-count

To specify the transmit hold count, use the **spanning-tree transmit hold-count** command. To return to the default settings, use the **no** form of this command.

**spanning-tree transmit hold-count** *value*

**no spanning-tree transmit hold-count**

<b>Syntax Description</b>	<i>value</i>	Number of BPDUs that can be sent before pausing for 1 second; valid values are from 1 to 20.
---------------------------	--------------	--

<b>Defaults</b>	<i>value</i> is 6.
-----------------	--------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	This command is supported on all spanning-tree modes. The transmit hold count determines the number of BPDUs that can be sent before pausing for 1 second.
-------------------------	---



**Note**

Changing this parameter to a higher value may have a significant impact on CPU utilization, especially in rapid-PVST mode. Lowering this parameter could slow convergence in some scenarios. We recommend that you do not change the value from the default setting.

If you change the *value* setting, enter the **show running-config** command to verify the change.

If you delete the command, use the **show spanning-tree mst** command to verify the deletion.

<b>Examples</b>	This example shows how to specify the transmit hold count:
-----------------	--

```
Router(config)# spanning-tree transmit hold-count 8
Router(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show running-config</b>	Displays the status and configuration of the module or Layer 2 VLAN.
	<b>show spanning-tree mst</b>	Displays the information about the MST protocol.

## spanning-tree uplinkfast

To enable UplinkFast, 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**]

<b>Syntax Description</b>	<b>max-update-rate</b> (Optional) Specifies the maximum rate (in packets per second) at which update packets are sent; valid values are from 0 to 65535. <i>packets-per-second</i>
---------------------------	---

<b>Defaults</b>	The defaults are as follows: <ul style="list-style-type: none"> <li>• UplinkFast is disabled.</li> <li>• <i>packets-per-second</i> is 150 packets per second.</li> </ul>
-----------------	--

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	<p>Use this command only on access switches.</p> <p>When you configure UplinkFast, the bridge priority is changed to 49152 so that this switch is not selected as root. All interface path costs of all spanning-tree interfaces that belong to the specified spanning-tree instances also increase by 3000.</p> <p>When spanning tree detects that the root interface has failed, UplinkFast causes an immediate switchover to an alternate root interface, transitioning the new root interface directly to the forwarding state. During this time, a topology change notification is sent. To minimize the disruption that is caused by the topology change, a multicast packet is sent to 01-00-0C-CD-CD-CD for each station address in the forwarding bridge except for those associated with the old root interface.</p> <p>Use the <b>spanning-tree uplinkfast max-update-rate</b> command to enable UplinkFast (if it is not already enabled) and change the rate at which update packets are sent. Use the <b>no</b> form of this command to return to the default rate.</p>
-------------------------	---

---

**Examples**

This example shows how to enable UplinkFast and set the maximum rate to 200 packets per second:

```
Router(config)# spanning-tree uplinkfast max-update-rate 200
Router(config)#
```

---

**Related Commands**

Command	Description
<a href="#">show spanning-tree</a>	Displays information about the spanning-tree state.

---

## spanning-tree vlan

To configure STP on a per-VLAN basis, use the **spanning-tree vlan** command. To return to the default settings, use the **no** form of this command.

```
spanning-tree vlan vlan-id [forward-time seconds | hello-time hello-time | max-age seconds |
priority priority | protocol protocol | {root {primary | secondary} [diameter net-diameter
hello-time hello-time]}]
```

```
no spanning-tree vlan vlan-id [forward-time | hello-time | max-age | priority | protocol | root]
```

### Syntax Description

<i>vlan-id</i>	VLAN identification number; valid values are from 1 to 4094.
<b>forward-time</b> <i>seconds</i>	(Optional) Specifies the STP forward-delay time; valid values are from 4 to 30 seconds.
<b>hello-time</b> <i>hello-time</i>	(Optional) Specifies the number of seconds between the generation of configuration messages by the root switch; valid values are from 1 to 10 seconds.
<b>max-age</b> <i>seconds</i>	(Optional) Specifies the maximum number of seconds that the information in a BPDU is valid; valid values are from 6 to 40 seconds.
<b>priority</b> <i>priority</i>	(Optional) Specifies the STP-bridge priority; valid values are from 0 to 65535.
<b>protocol</b> <i>protocol</i>	(Optional) Specifies the STP; see the “Usage Guidelines” section for a list of valid values.
<b>root primary</b>	(Optional) Forces this switch to be the root bridge.
<b>root secondary</b>	(Optional) Forces this switch to be the root switch should the primary root fail.
<b>diameter</b> <i>net-diameter</i>	(Optional) Specifies the maximum number of bridges between any two points of attachment between end stations; valid values are from 2 through 7.

### Defaults

The defaults are as follows:

- **forward-time**—15 seconds
- **hello-time**—2 seconds
- **max-age**—20 seconds
- **priority**—The default with IEEE STP enabled is 32768; the default with STP enabled is 128
- **protocol**—IEEE
- **root**—No STP root

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

---

**Usage Guidelines****Caution**

---

When disabling spanning tree on a VLAN using the **no spanning-tree vlan** *vlan-id* command, ensure that all switches and bridges in the VLAN have spanning tree disabled. You cannot disable spanning tree on some switches and bridges in a VLAN and leave it enabled on other switches and bridges in the same VLAN because switches and bridges with spanning tree enabled have incomplete information about the physical topology of the network.

---

**Caution**

---

We do not recommend disabling spanning tree, even in a topology that is free of physical loops. Spanning tree is a safeguard against misconfigurations and cabling errors. Do not disable spanning tree in a VLAN without ensuring that there are no physical loops present in the VLAN.

---

When setting the **max-age** *seconds*, 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.

Valid values for *protocol* are **dec**—Digital STP, **ibm**—IBM STP, **ieee**—IEEE Ethernet STP, and **vlan-bridge**—VLAN Bridge STP.

The **spanning-tree root primary** alters this switch's 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 results.

The **spanning-tree root secondary** alters this switch's bridge priority to 16384. If the root switch should fail, this switch becomes the next root switch.

Use the **spanning-tree root** commands on the backbone switches only.

---

**Examples**

This example shows how to enable spanning tree on VLAN 200:

```
Router(config)# spanning-tree vlan 200
Router(config)#
```

This example shows how to configure the switch as the root switch for VLAN 10 with a network diameter of 4:

```
Router(config)# spanning-tree vlan 10 root primary diameter 4
Router(config)#
```

This example shows how to configure the switch as the secondary root switch for VLAN 10 with a network diameter of 4:

```
Router(config)# spanning-tree vlan 10 root secondary diameter 4
Router(config)#
```

---

**Related Commands**

---

Command	Description
<a href="#">show spanning-tree</a>	Displays information about the spanning-tree state.

---

# speed

To set the port speed for an Ethernet interface, use the **speed** command. To disable a speed setting, use the **no** form of this command.

**speed** { **10** | **100** | **1000** }

**speed auto** [*speed-list*]

**speed** [**1000** | **nonegotiate**]

**no speed**

Syntax Description		
<b>10</b>	Specifies the interface transmits at 10 Mbps.	
<b>100</b>	Specifies the interface transmits at 100 Mbps.	
<b>1000</b>	(Optional) Specifies the interface transmits at 1000 Mbps.	
<b>auto</b>	Enables the autonegotiation capability.	
<i>speed-list</i>	(Optional) Speed autonegotiation capability to a specific speed; see the “Usage Guidelines” section for valid values.	
<b>nonegotiate</b>	(Optional) Enables or disables the link-negotiation protocol on the Gigabit Ethernet ports.	

**Defaults** See [Table 2-93](#) for a list of default settings.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Use the **speed** [**10** | **100**] command for 10/100 ports, the **speed auto** [**10 100** [**1000**]] command for 10/100/1000 ports, and the **speed** [**1000** | **nonegotiate**] command for Gigabit Ethernet ports.

Separate the *speed-list* entries with a space.

The following *speed-list* configurations are supported:

- **speed auto**—Negotiate all speeds.
- **speed auto 10 100**—Negotiate 10 and 100 speeds only.
- **speed auto 10 100 1000**—Negotiate all speeds.

When you enable link negotiation, the speed, duplex, flow control, and clocking negotiations between two Gigabit Ethernet ports are automatically enabled.

Table 2-93 lists the supported command options by interface.

**Table 2-93 Supported speed Command Options**

Interface Type	Supported Syntax	Default Setting	Usage Guidelines
10/100-Mbps module	<b>speed [10   100]</b> <b>speed auto [10   100]</b>	<b>auto</b>	If the speed is set to <b>auto</b> , you cannot set <b>duplex</b> .  If the speed is set to <b>10</b> or <b>100</b> , and you do not configure the duplex setting, the duplex is set to <b>half</b> .
10/100/1000-Mbps interface	<b>speed auto [{ 10 100 } [1000]]</b>	<b>auto</b>	If the speed is set to <b>auto</b> , you cannot set <b>duplex</b> .  If the speed is set to <b>10</b> or <b>100</b> , and you do not configure the duplex setting, the duplex is set to <b>half</b> by default.  If the speed is set to <b>10 100</b> , the interface is not forced to half duplex by default.
100-Mbps fiber modules	Factory set	Not applicable.	
Gigabit Ethernet module	<b>speed [1000   nonegotiate]</b>	Speed is 1000 or negotiation is enabled.	Speed, duplex, flow control, and clocking negotiations are enabled.
10-Mbps ports	Factory set	Not applicable.	

If you decide to configure the interface speed and duplex commands manually, and enter a value other than **speed auto** (for example, 10 or 100 Mbps), ensure that you configure the connecting interface speed command to a matching speed but do not use the **auto** keyword.

If you set the Ethernet interface speed to **auto** on a 10/100-Mbps or 10/100/1000-Mbps Ethernet interface, both speed and duplex are autonegotiated.

The Gigabit Ethernet interfaces are full duplex only. You cannot change the duplex mode on the Gigabit Ethernet interfaces or on a 10/100/1000-Mbps interface that is configured for Gigabit Ethernet.

When manually configuring the interface speed to either 10 or 100 Mbps, the switch prompts you to configure duplex mode on the interface.



**Note**

Catalyst 6500 series switches cannot automatically negotiate interface speed and duplex mode if either connecting interface is configured to a value other than **auto**.



**Caution**

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

You cannot set the duplex mode to **half** when the port speed is set at 1000 and similarly, you cannot set the port speed to **1000** when the mode is set to half duplex. In addition, if the port speed is set to **auto**, the **duplex** command is rejected.

Table 2-94 describes the relationship between the **duplex** and **speed** commands.

*Table 2-94 Relationship Between duplex and speed Commands*

duplex Command	speed Command	Resulting System Action
<b>duplex half</b> or <b>duplex full</b>	<b>speed auto</b>	Autonegotiates both speed and duplex modes
<b>duplex half</b>	<b>speed 10</b>	Forces 10 Mbps and half duplex
<b>duplex full</b>	<b>speed 10</b>	Forces 10 Mbps and full duplex
<b>duplex half</b>	<b>speed 100</b>	Forces 100 Mbps and half duplex
<b>duplex full</b>	<b>speed 100</b>	Forces 100 Mbps and full duplex
<b>duplex full</b>	<b>speed 1000</b>	Forces 1000 Mbps and full duplex

### Examples

This example shows how to configure the interface to transmit at 100 Mbps:

```
Router(config-if)# speed 100
Router(config-if)#
```

### Related Commands

Command	Description
<b>duplex</b>	Configures the duplex operation on an interface.
<b>interface</b>	Selects an interface to configure and enters interface configuration mode.
<b>show interfaces</b>	Displays traffic that is seen by a specific interface.

# squeeze

To delete flash files permanently by squeezing a flash file system, use the **squeeze** command.

**squeeze** *filesystem:*

<b>Syntax Description</b>	<i>filesystem:</i> Flash file system; valid values are <b>bootflash:</b> and <b>flash:</b> .
---------------------------	--

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	When flash memory is full, you might need to rearrange the files so that the space that is used by the files that are marked “deleted” can be reclaimed.
-------------------------	--

When you enter the **squeeze** command, the router copies all valid files to the beginning of flash memory and erases all files that are marked “deleted.” You cannot recover “deleted” files and you can write to the reclaimed flash-memory space.

In addition to removing deleted files, use the **squeeze** command to remove any files that the system has marked as “error.” An error file is created when a file write fails (for example, the device is full). To remove error files, you must use the **squeeze** command. The squeeze operation might take as long as several minutes because it can involve erasing and rewriting almost an entire flash-memory space.

The colon is required when entering the *filesystem*.

<b>Examples</b>	This example shows how to permanently erase the files that are marked “deleted” from the flash memory:
-----------------	--

```
Router # squeeze flash:
Router #
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>delete</b>	Deletes a file from a flash memory device or NVRAM.
	<b>dir</b>	Displays a list of files on a file system.
	<b>undelete</b>	Recovers a file that is marked “deleted” on a flash file system.

## stack-mib portname

To specify a name string for a port, use the **stack-mib portname** command.

**stack-mib portname** *portname*

<b>Syntax Description</b>	<i>portname</i> Name for a port.
---------------------------	----------------------------------

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	Using the <b>stack-mib</b> command to set a name string to a port corresponds to the portName MIB object in the portTable of CISCO-STACK-MIB. portName is the MIB object in the portTable of CISCO-STACK-MIB. You can set this object to be descriptive text describing the function of the interface.
-------------------------	--

<b>Examples</b>	This example shows how to set a name to a port:
-----------------	---

```
Router(config-if)# stack-mib portname portal_to_paradise
Router(config-if)#
```

# standby delay minimum reload

To configure the delay period before the initialization of HSRP groups, use the **standby delay minimum reload** command. To disable the delay period, use the **no** form of this command.

**standby delay minimum** [*min-delay*] **reload** [*reload-delay*]

**no standby delay minimum** [*min-delay*] **reload** [*reload-delay*]

Syntax Description		
<i>min-delay</i>	(Optional) Minimum time, in seconds, to delay HSRP-group initialization after an interface comes up. This minimum delay applies to all subsequent interface events.	
<i>reload-delay</i>	(Optional) Time, in seconds, to delay after the router has reloaded. This delay applies only to the first interface-up event after the router has reloaded.	

## Defaults

The defaults are as follows:

- *min-delay* is **1** second.
- *reload-delay* is **5** seconds.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

If the active router fails or is removed from the network, the standby router automatically becomes the new active router. If the former active router comes back online, you can control whether it takes over as the active router by using the **standby preempt** command.

However, even if the **standby preempt** command is not configured, the former active router resumes the active role after it reloads and comes back online. Use the **standby delay minimum reload** command to set a delay period for HSRP-group initialization. This command allows time for the packets to get through before the router resumes the active role.

We recommend that you use the **standby delay minimum reload** command if the **standby timers** command is configured in milliseconds or if HSRP is configured on a VLAN interface of a switch.

In most configurations, the default values provide sufficient time for the packets to get through, and it is not necessary to configure longer delay values.

The delay is canceled if an HSRP packet is received on an interface.

**Examples**

This example shows how to set the minimum delay to 30 seconds and the delay after the first reload to 120 seconds:

```
Router(config-if) # standby delay minimum 30 reload 120
Router(config-if) #
```

**Related Commands**

Command	Description
<a href="#">show standby delay</a>	Displays HSRP information about the delay periods.
<b>standby preempt</b>	Configures HSRP preemption and preemption delay.
<b>standby timers</b>	Configures the time between hello packets and the time before other routers declare the active Hot Standby or standby router to be down.

# standby track

To configure an interface so that the Hot Standby-priority changes are based on the availability of other interfaces, use the **standby track** command. To delete all tracking configuration for a group, use the **no** form of this command.

```
standby [group-number] track {interface-type interface-number | designated-router}
[priority-decrement]
```

```
no standby group-number track
```

Syntax Description	
<i>group-number</i>	(Optional) Group number on the interface to which the tracking applies; valid values are from 0 to 255.
<i>interface-type</i> <i>interface-number</i>	Interface type and number to be tracked.
<b>designated-router</b>	Specifies that if the designated router becomes nondesignated, the active HSRP router becomes the designated router.
<i>priority-decrement</i>	(Optional) Amount that the Hot Standby priority for the router is decremented (or incremented) when the interface goes down (or comes back up); valid values are from 1 to 255.

## Defaults

The defaults are as follows:

- The *group* is **0**.
- The *priority-decrement* is **10**.
- The **designated-router** keyword is disabled.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

Prior to entering the **designated-router** keyword, you must ensure that the new designated router has a higher HSRP priority than the current designated router to take over.

When a tracked interface goes down, the Hot Standby priority decreases by the number that is specified by the *priority-decrement* argument. If an interface is not tracked, its state changes do not affect the Hot Standby priority. For each interface that is configured for Hot Standby, you can configure a separate list of interfaces to be tracked.

When multiple tracked interfaces are down, the decrements are cumulative whether they are configured with *priority-decrement* values or not.

A tracked interface is considered down if the IP address is disabled on that interface.

You must enter the *group-number* when using the **no** form of this command.

If you configure HSRP to track an interface, and that interface is physically removed as in the case of an OIR operation, then HSRP regards the interface as always down. You cannot remove the HSRP interface-tracking configuration. To prevent this situation, use the **no standby track interface-type interface-number** command before you physically remove the interface.

When you enter a *group-number* **0**, no group number is written to NVRAM, providing backward compatibility.

---

### Examples

This example shows how to enable HSRP tracking for group 1 on an interface:

```
Router(config-if)# standby 1 track Ethernet0/2
Router(config-if)#
```

This example shows how to specify that if the designated router becomes nondesignated, the active HSRP router becomes the designated router:

```
Router(config-if)# standby 1 track designated-router 15
Router(config-if)#
```

---

### Related Commands

Command	Description
<b>show standby</b>	Displays HSRP information.

## standby use-bia

To configure the HSRP to use the burned-in address of the interface as its virtual MAC address instead of the preassigned MAC address (on Ethernet and FDDI) or the functional address (on Token Ring), use the **standby use-bia** command. To return to the default virtual MAC address, use the **no** form of this command.

**standby use-bia** [**scope interface**]

**no standby use-bia**

<b>Syntax Description</b>	<b>scope interface</b> (Optional) Configures this command for the subinterface on which it was entered instead of the major interface.
---------------------------	--

<b>Defaults</b>	HSRP uses the preassigned MAC address on Ethernet and FDDI or the functional address on Token Ring.
-----------------	---

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

<b>Command History</b>	<table border="1"> <thead> <tr> <th style="border: none;">Release</th> <th style="border: none;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border: none;">12.2(18)ZY</td> <td style="border: none;">Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)ZY	Support for this command was introduced.
Release	Modification				
12.2(18)ZY	Support for this command was introduced.				

<b>Usage Guidelines</b>	<p>This command is not supported on Catalyst 6500 series switches that are configured with a PFC2. The PFC2 supports a maximum of 16 unique HSRP-group numbers. You can use the same HSRP-group numbers in different VLANs. If you configure more than 16 HSRP groups, this restriction prevents use of the VLAN number as the HSRP-group number.</p>
-------------------------	---



<b>Note</b>	Identically numbered HSRP groups use the same virtual MAC address, which might cause errors if you configure bridge groups.
-------------	---

Hardware Layer 3 switching supports the following ingress and egress encapsulations:

- Ethernet V2.0 (ARPA)
- 802.3 with 802.2 with 1 byte control (SAP1)
- 802.3 with 802.2 and SNAP

Hardware Layer 3 switching is permanently enabled. No configuration is required.

<b>Examples</b>	This example shows how to configure the HSRP to use the burned-in address of the interface as the virtual MAC address that is mapped to the virtual IP address:
-----------------	---

```
Router(config-if) # standby use-bia
Router(config-if) #
```

## storm-control level

To set the suppression level, use the **storm-control level** command. To turn off the suppression mode, use the **no** form of this command.

**storm-control** { **broadcast** | **multicast** | **unicast** } **level** *level* [*.level*]

**no storm-control** { **broadcast** | **multicast** | **unicast** } **level**

Syntax Description		
	<b>broadcast</b>	Specifies the broadcast traffic.
	<b>multicast</b>	Specifies the multicast traffic.
	<b>unicast</b>	Specifies the unicast traffic.
	<i>level</i>	Integer-suppression level; valid values are from 0 to 100 percent.
	<i>.level</i>	(Optional) Fractional-suppression level; valid values are from 0 to 99.

**Defaults** All packets are passed.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** You can enter this command on switch ports and router ports.

Enter the **storm-control level** command to enable traffic storm control on the interface, configure the traffic storm-control level, and apply the traffic storm-control level to all traffic storm-control modes that are enabled on the interface.

Only one suppression level is shared by all three suppression modes. For example, if you set the broadcast level to 30 and set the multicast level to 40, both levels are enabled and set to 40.

The Catalyst 6500 series switch supports storm control for multicast and unicast traffic only on Gigabit and 10-Gigabit Ethernet LAN ports. The switch supports storm control for broadcast traffic on all LAN ports.

The **multicast** and **unicast** keywords are supported on Gigabit and 10-Gigabit Ethernet LAN ports only. Unicast and multicast suppression is also supported on the WS-X6148A-RJ-45 and the WS-X6148-SFP modules.

The period is required when you enter the fractional-suppression level.

The suppression level is entered as a percentage of the total bandwidth. A threshold value of 100 percent means that no limit is placed on traffic. A threshold value of 0 or 0.0 (fractional) percent means that all specified traffic is blocked on a port, with the following guidelines:

- A fractional level value of 0.33 or lower is the same as 0.0 on the following modules:
  - WS-X6704-10GE
  - WS-X6748-SFP
  - WS-X6724-SFP
  - WS-X6748-GE-TX
- Enter 0 on all other modules to block all specified traffic on a port.

Enter the **show interfaces counters broadcast** 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 *level* to 100 percent for the specified traffic type.
- Use the **no** form of this command.

### Examples

This example shows how to enable and set the suppression level:

```
Router(config-if)# storm-control broadcast level 30
Router(config-if)#
```

This example shows how to disable the suppression mode:

```
Router(config-if)# no storm-control multicast level
Router(config-if)#
```

### Related Commands

Command	Description
<b>show interfaces counters</b>	Displays the traffic that the physical interface sees.
<b>show running-config</b>	Displays the status and configuration of the module or Layer 2 VLAN.

# switchport

To modify the switching characteristics of the Layer 2-switched interface, use the **switchport** command (without parameters). 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). Use the **switchport** commands (with parameters) to configure the switching characteristics.

**switchport**

**switchport {host | nonegotiate}**

**no switchport**

**no switchport nonegotiate**

## Syntax Description

<b>host</b>	Optimizes the port configuration for a host connection.
<b>nonegotiate</b>	Specifies that the device will not engage in a negotiation protocol on this interface.

## Defaults

The default access VLAN and trunk-interface native VLAN are default VLANs that correspond to the platform or interface hardware.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## 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 additional **switchport** commands with keywords. This action is required only if you have not entered the **switchport** command for the interface.

Entering the **no switchport** command shuts down the port and then reenables it. This action may generate messages on the device to which the port is connected.

To optimize the port configuration, entering the **switchport host** command sets the switch port mode to access, enables spanning tree PortFast, and disables channel grouping. Only an end station can accept this configuration.

Because spanning-tree PortFast is enabled, you should enter the **switchport host** command only on ports that are connected to a single host. Connecting other Catalyst 6500 series switches, hubs, concentrators, switches, and bridges to a fast-start port can cause temporary spanning-tree loops.

Enable the **switchport host** command to decrease the time that it takes to start up packet forwarding.

The **no** form of the **switchport nonegotiate** command removes **nonegotiate** status.

When using the **nonegotiate** keyword, DISL/DTP-negotiation packets are not sent on the interface. The device trunks or does not trunk according to the **mode** parameter given: **access** or **trunk**. This command returns an error if you attempt to execute it in **dynamic (auto or desirable)** mode.

You must force a port to trunk before you can configure it as a SPAN-destination port. Use the **switchport nonegotiate** command to force the port to trunk.

### 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:

```
Router(config-if)# switchport
Router(config-if)#
```



### 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.

This example shows how to optimize the port configuration for a host connection:

```
Router(config-if)# switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
Router(config-if)#
```

This example shows how to cause a port interface that has already been configured as a switched interface to refrain from negotiating trunking mode and act as a trunk or access port (depending on the **mode** set):

```
Router(config-if)# switchport nonegotiate
Router(config-if)#
```

### Related Commands

Command	Description
<a href="#">show interfaces</a> <a href="#">switchport</a>	Displays the administrative and operational status of a switching (nonrouting) port.

# switchport access vlan

To set the VLAN when the 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*

**no switchport access vlan**

Syntax Description	<i>vlan-id</i>	VLAN to set when the interface is in access mode; valid values are from 1 to 4094.
--------------------	----------------	--

## Defaults

The defaults are as follows:

- Access VLAN and trunk-interface native VLAN are default VLANs that correspond to the platform or interface hardware.
- All VLAN lists include all VLANs.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

You must enter the **switchport** command without any keywords to configure the LAN interface as a Layer 2 interface before you can enter the **switchport access vlan** command. This action is required only if you have not entered the **switchport** command for the interface.

Entering the **no switchport** command shuts down the port and then reenables it. This action may generate messages on the device to which the port is connected.

The **no** form of the **switchport access vlan** command resets the access-mode VLAN to the appropriate default VLAN for the device.

**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:

```
Router(config-if)# switchport
Router(config-if)#
```

**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.

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 in the interface-configuration mode:

```
Router(config-if)# switchport access vlan 2
Router(config-if)#
```

**Related Commands**

Command	Description
<a href="#">show interfaces</a>	Displays the administrative and operational status of a switching (nonrouting) port.
<a href="#">switchport</a>	

# 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**

**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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**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.

A VLAN interface configured on the PISA is considered up if there are ports forwarding in the associated VLAN. When all ports on a VLAN are down or blocking, the VLAN interface on the PISA is considered down. For the VLAN interface to be considered up, all the ports in the VLAN need to be up and forwarding. You can enter the **switchport autostate exclude** command to exclude a port from the VLAN interface link-up calculation.

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.

The **show interface *interface* switchport** command displays the autostate mode if the mode has been set. If the mode has not been set, the autostate mode is not displayed.

---

**Examples**

This example shows how to exclude a port from the VLAN interface link-up calculation:

```
Router(config-if)# switchport autostate exclude  
Router(config-if)#
```

This example shows how to include a port in the VLAN interface link-up calculation:

```
Router(config-if)# no switchport autostate exclude  
Router(config-if)#
```

---

**Related Commands**

Command	Description
<a href="#">show interfaces switchport</a>	Displays the administrative and operational status of a switching (nonrouting) port.

# switchport backup

To configure an interface as a Flexlink backup interface, use the **switchport backup** command. To disable Flexlink, use the **no** form of this command.

**switchport backup interface** *interface-type interface-number*

**no switchport backup interface** *interface-type interface-number*

Syntax Description	<b>interface</b> <i>interface-type interface-number</i> Specifies the interface type and the module and port number to configure as a Flexlink backup interface.				
Defaults	Disabled				
Command Modes	Interface configuration				
Command History	<table border="1"> <thead> <tr> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Release</th> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border-bottom: 1px solid black;">12.2(18)ZY</td> <td style="border-bottom: 1px solid black;">Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)ZY	Support for this command was introduced.
Release	Modification				
12.2(18)ZY	Support for this command was introduced.				
Usage Guidelines	<p>When you enable Flexlink, both the active and the standby links are up physically and mutual backup is provided.</p> <p>Flexlink is supported on Layer 2 interfaces only and does not support routed ports.</p> <p>Flexlink does not switch back to the original active interface after recovery.</p> <p>The <i>interface-number</i> designates the module and port number. Valid values depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 1 to 13 and valid values for the port number are from 1 to 48.</p> <p>Flexlink is designed for simple access topologies (two uplinks from a leaf node). You must ensure that there are no loops from the wiring closet to the distribution/core network to enable Flexlink to perform correctly.</p> <p>Flexlink converges faster for directly connected link failures only. Any other network failure has no improvement with Flexlink fast convergence.</p> <p>You must enter the <b>switchport</b> command without any keywords to configure the LAN interface as a Layer 2 interface before you can enter the <b>switchport autostate exclude</b> command. This action is required only if you have not entered the <b>switchport</b> command for the interface.</p>				
 Note	<p>The <b>switchport</b> 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.</p>				

---

**Examples**

This example shows how to enable Flexlink on an interface:

```
Router(config-if)# switchport backup interface fastethernet 4/1  
Router(config-if)#
```

This example shows how to disable Flexlink on an interface:

```
Router(config-if)# switchport backup interface fastethernet 4/1  
Router(config-if)#
```

---

**Related Commands**

Command	Description
<a href="#">show interfaces</a>	Displays Flexlink pairs.
<a href="#">switchport backup</a>	

---

# switchport block unicast

To prevent the unknown unicast packets from being forwarded, use the **switchport block unicast** command. To allow the unknown unicast packets to be forwarded, use the **no** form of this command.

**switchport block unicast**

**no switchport block unicast**

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

**Defaults** The default settings are as follows:

- Unknown unicast traffic is not blocked.
- All traffic with unknown MAC addresses is sent to all ports.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** You can block the unknown unicast traffic on the switch ports.

Blocking the unknown unicast traffic is not automatically enabled on the switch ports; you must explicitly configure it.



**Note**

For more information about blocking the packets, refer to the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*.

You can verify your setting by entering the **show interfaces interface-id switchport** command.

**Examples** This example shows how to block the unknown unicast traffic on an interface:

```
Router(config-if)# switchport block unicast
Router(config-if)#
```

Related Commands	Command	Description
	<a href="#">show interfaces switchport</a>	Displays the administrative and operational status of a switching (nonrouting) port.

# switchport capture

To configure the port to capture VACL-filtered traffic, use the **switchport capture** command. To disable the capture mode on the port, use the **no** form of this command.

**switchport capture**

**no switchport capture**

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

**Defaults** Disabled

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** You must enter the **switchport** command without any keywords to configure the LAN interface as a Layer 2-switched interface before you can enter additional **switchport** commands with keywords. This action is required only if you have not entered the **switchport** command for the interface.

The VACL capture function for the NAM is supported on the Supervisor Engine 720 but is not supported with the IDSM-2.

The **switchport capture** command applies only to Layer 2-switched interfaces.

WAN interfaces support only the capture functionality of VACLs.

Entering the **no switchport** command shuts down the port and then reenables it. This action may generate messages on the device to which the port is connected.

Entering the **switchport capture** command sets the capture function on the interface so that the packets with the capture bit set are received by the interface.

There is no restriction on the order that you enter the **switchport capture** and **switchport capture allowed vlan** commands. The port does not become a capture port until you enter the **switchport capture** (with no arguments) command.

The capture port must allow the destination VLANs of the captured packets. Once you enable a capture port, the packets are allowed from all VLANs by default, the capture port is no longer in the originally configured mode, and the capture mode enters monitor mode. In monitor mode, the capture port does the following:

- Does not belong to any VLANs that it was in previously.
- Does not allow incoming traffic.

- Preserves the encapsulation on the capture port if you enable the capture port from a trunk port and the trunking encapsulation was ISL or 802.1Q. The captured packets are encapsulated with the corresponding encapsulation type. If you enable the capture port from an access port, the captured packets are not encapsulated.
- When you enter the **no switchport capture** command to disable the capture function, the port returns to the previously configured mode (access or trunk).
- Packets are captured only if the destination VLAN is allowed on the capture port.

---

### Examples

This example shows how to configure an interface to capture VACL-filtered traffic:

```
Router(config-if)# switchport capture
Router(config-if)#
```

---

### Related Commands

Command	Description
<a href="#">show interfaces switchport</a>	Displays the administrative and operational status of a switching (nonrouting) port.
<a href="#">switchport capture allowed vlan</a>	Specifies the destination VLANs of the VACL-filtered traffic.

## switchport capture allowed vlan

To specify the destination VLANs of the VACL-filtered traffic, use the **switchport capture allowed vlan** command. To clear the configured-destination VLAN list and return to the default settings, use the **no** form of this command.

```
switchport capture allowed vlan {add | all | except | remove} vlan-id [,vlan-id[,vlan-id[,...]]
```

```
no switchport capture allowed vlan
```

### Syntax Description

<b>add</b>	Adds the specified VLANs to the current list.
<b>all</b>	Adds all VLANs to the current list.
<b>except</b>	Adds all VLANs except the ones that are specified.
<b>remove</b>	Removes the specified VLANs from the current list.
<i>vlan-id</i>	VLAN IDs of the allowed VLANs when this port is in capture mode; valid values are from 1 to 4094.

### Defaults

**all**

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

You must enter the **switchport** command without any keywords to configure the LAN interface as a Layer 2-switched interface before you can enter additional **switchport** commands with keywords. This action is required only if you have not entered the **switchport** command for the interface.

The **switchport capture allowed vlan** command applies only to Layer 2-switched interfaces.

Entering the **no switchport** command shuts down the port and then reenables it. This action may generate messages on the device to which the port is connected.

You can enter the *vlan-id* as a single VLAN, a group of VLANs, or both. For example, you would enter **switchport capture allowed vlan 1-1000, 2000, 3000-3100**.

There is no restriction on the order that you enter the **switchport capture** and **switchport capture allowed vlan** commands. The port does not become a capture port until you enter the **switchport capture** (with no arguments) command.

WAN interfaces support only the capture functionality of VACLs.

**switchport capture allowed vlan****Examples**

This example shows how to add the specified VLAN to capture VACL-filtered traffic:

```
Router(config-if)# switchport capture allowed vlan add 100  
Router(config-if)#
```

**Related Commands**

Command	Description
<a href="#">show interfaces switchport</a>	Displays the administrative and operational status of a switching (nonrouting) port.

# switchport dot1q ethertype

To specify the EtherType value to be programmed on the interface, use the **switchport dot1q ethertype** command. To return to the default settings, use the **no** form of this command.

**switchport dot1q ethertype** *value*

<b>Syntax Description</b>	<i>value</i> EtherType value for 802.1Q encapsulation; valid values are from 0x600 to 0xFFFF.
---------------------------	---

<b>Defaults</b>	The <i>value</i> is 0x8100.
-----------------	-----------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** You can configure a custom EtherType-field value on trunk ports and on access ports. Each port supports only one EtherType-field value. A port that is configured with a custom EtherType-field value does not recognize frames that have any other EtherType-field value as tagged frames.



### Caution

A port that is configured with a custom EtherType-field value considers frames that have any other EtherType-field value to be untagged frames. A trunk port that is configured with a custom EtherType-field value puts frames that are tagged with any other EtherType-field value into the native VLAN. An access port or tunnel port that is configured with a custom EtherType-field value puts frames that are tagged with any other EtherType-field value into the access VLAN.

You can configure a custom EtherType-field value on the following modules:

- Supervisor engines
- WS-X6516A-GBIC
- WS-X6516-GBIC



**Note** The WS-X6516A-GBIC and WS-X6516-GBIC modules apply a configured custom EtherType-field value to all ports that are supported by each port ASIC (1 through 8 and 9 through 16).

- WS-X6516-GE-TX

You cannot configure a custom EtherType-field value on the ports in an EtherChannel.

You cannot form an EtherChannel from ports that are configured with custom EtherType-field values.

## ■ switchport dot1q etherType

---

**Examples**

This example shows how to set the EtherType value to be programmed on the interface:

```
Router (config-if)# switchport dot1q etherType 1234  
Router (config-if)#
```

---

**Related Commands**

Command	Description
<a href="#">show interfaces switchport</a>	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 | trunk | {dynamic {auto | desirable}} | dot1q-tunnel}

**switchport mode private-vlan** {host | promiscuous}

**no switchport mode**

**no switchport mode private-vlan**

Syntax Description	access	Specifies the nontrunking, nontagged single-VLAN Layer-2 interface.
	<b>trunk</b>	Specifies the trunking VLAN interface in Layer 2.
	<b>dynamic auto</b>	Specifies the interface that converts the link to a trunk link.
	<b>dynamic desirable</b>	Specifies the interface that actively attempts to convert the link to a trunk link.
	<b>dot1q-tunnel</b>	Specifies the 802.1Q-tunneling interface.
	<b>private-vlan host</b>	Specifies the ports with a valid PVLAN association that become active host-PVLAN ports.
	<b>private-vlan promiscuous</b>	Specifies the ports with a valid PVLAN mapping that become active promiscuous ports.

## Defaults

The defaults are as follows:

- The mode is dependent on the platform; it should either be **dynamic auto** for platforms that are intended for wiring closets or **dynamic desirable** for platforms that are intended as backbone switches.
- No mode is set for PVLAN ports.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## 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 agree to 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 agree to 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 configure a port as a promiscuous or host-PVLAN port and one of the following applies, the port becomes inactive:

- The port does not have a valid PVLAN association or mapping configured.
- The port is a SPAN destination.

If you delete a private-port PVLAN association or mapping, or if you configure a private port as a SPAN destination, the deleted private-port PVLAN association or mapping or the private port that is configured as a SPAN destination becomes inactive.

If you enter **dot1q-tunnel** mode, BPDU filtering is enabled and CDP is disabled on protocol-tunneled interfaces.

### Examples

This example shows how to set the interface to dynamic desirable mode:

```
Router(config-if)# switchport mode dynamic desirable
Router(config-if)#
```

This example shows how to set a port to PVLAN-host mode:

```
Router(config-if)# switchport mode private-vlan host
Router(config-if)#
```

This example shows how to set a port to PVLAN-promiscuous mode:

```
Router(config-if)# switchport mode private-vlan promiscuous
Router(config-if)#
```

### Related Commands

Command	Description
<a href="#">show dot1q-tunnel</a>	Displays a list of 802.1Q tunnel-enabled ports.
<a href="#">show interfaces switchport</a>	Displays the administrative and operational status of a switching (nonrouting) port.
<a href="#">switchport</a>	Modifies the switching characteristics of the Layer 2-switched interface.
<a href="#">switchport private-vlan host-association</a>	Modifies the switching characteristics of the Layer 2-switched interface.
<a href="#">switchport private-vlan mapping</a>	Defines the PVLAN 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, use the **no** form of this command.

**switchport port-security**

**no switchport port-security**

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

**Defaults** Disabled

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Follow these guidelines when configuring port security:

- Port security is supported on trunks.
- Port security is supported on 802.1Q tunnel ports.
- A secure port cannot be a destination port for a Switch Port Analyzer (SPAN).
- A secure port cannot belong to an EtherChannel.
- A secure port cannot be a trunk port.
- A secure port cannot be an 802.1X port. If you try to enable 802.1X on a secure port, an error message appears, and 802.1X is not enabled. If you try to change an 802.1X-enabled port to a secure port, an error message appears, and the security settings are not changed.

**Examples** This example shows how to enable port security:

```
Router(config-if)# switchport port-security
Router(config-if)#
```

This example shows how to disable port security:

```
Router(config-if)# no switchport port-security
Router(config-if)#
```

Related Commands	Command	Description
	<a href="#">show port-security</a>	Displays information about the port-security setting.

## switchport port-security aging

To configure the port security aging, use the **switchport port-security aging** command. To disable aging, use the **no** form of this command.

**switchport port-security aging** {{ **time** *time* } | { **type** { **absolute** | **inactivity** } } }

Syntax Description	Parameter	Description
	<b>time</b> <i>time</i>	Sets the duration for which all addresses are secured; valid values are from 1 to 1440 minutes.
	<b>type</b>	Specifies the type of aging.
	<b>absolute</b>	Specifies absolute aging; see the “Usage Guidelines” section for more information.
	<b>inactivity</b>	Specifies that the timer starts to run only when there is no traffic; see the “Usage Guidelines” section for more information.

### Defaults

The defaults are as follows:

- Disabled
- If enabled, the defaults are as follows:
  - *time* is 0.
  - **type** is **absolute**.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

Follow these guidelines when configuring port security:

- Port security is supported on trunks.
- Port security is supported on 802.1Q tunnel ports.
- You can apply one of two types of aging for automatically learned addresses on a secure port:
- Absolute aging times out the MAC address after the age-time has been exceeded, regardless of the traffic pattern. This default is for any secured port, and the age-time is set to 0.
- Inactivity aging times out the MAC address only after the age\_time of inactivity from the corresponding host has been exceeded.

### Examples

This example shows how to set the aging time as 2 hours:

```
Router(config-if)# switchport port-security aging time 120
Router(config-if)#
```

This example shows how to set the aging time as 2 minutes:

```
Router(config-if)# switchport port-security aging time 2
Router(config-if)#
```

This example shows how to set the aging type on a port to absolute aging:

```
Router(config-if) switchport port-security aging type absolute
Router(config-if)#
```

This example shows how to set the aging type on a port to inactivity:

```
Router(config-if) switchport port-security aging type inactivity
Router(config-if)#
```

---

**Related Commands**

Command	Description
<a href="#">show port-security</a>	Displays information about the port-security setting.

---

# switchport port-security mac-address

To add a MAC address to the list of secure MAC addresses, use the **switchport port-security mac-address** command. To remove a MAC address from the list of secure MAC addresses, use the **no** form of this command.

**switchport port-security mac-address** {*mac-addr* | {**sticky** [*mac-addr*]}} [**vlan** *vlan* | *vlan-list*]

**no switchport port-security mac-address** *mac-addr* [**vlan** *vlan* | *vlan-list*]

Syntax Description		
<i>mac-addr</i>	MAC addresses for the interface; valid values are from 1 to 1024.	
<b>sticky</b>	Configures the dynamic MAC addresses as sticky on an interface.	
<b>vlan</b> <i>vlan</i>   <i>vlan-list</i>	(Optional) Specifies a VLAN or range of VLANs; see the “Usage Guidelines” section for additional information.	

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

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** If you configure fewer secure MAC addresses than the maximum number of secure MAC addresses on all interfaces, the remaining MAC addresses are dynamically learned.

To clear multiple MAC addresses, you must enter the **no** form of this command once for each MAC address to be cleared.

The *vlan-list* argument is visible only if the port has been configured and is operational as a trunk. Enter the **switchport mode trunk** command and then enter the **switchport nonegotiate** command.

The **sticky** keyword configures the dynamic MAC addresses as sticky on an interface. Sticky MAC addresses configure the static Layer 2 entry to stay sticky to a particular interface. This feature can prevent MAC moves or prevent the entry from being learned on a different interface.

You can configure the sticky feature even when port security is not enabled on the interface. It becomes operational once port security is enabled on the interface.



#### Note

You can enter the **switchport port-security mac-address sticky** command only if the sticky feature is enabled on the interface.

When port security is enabled, disabling the sticky feature causes all configured and learned sticky addresses to be deleted from the configuration and converted into dynamic secure addresses.

When port security is disabled, disabling the sticky feature causes all configured and learned sticky addresses to be deleted from the configuration.

**Examples**

This example shows how to configure a secure MAC address:

```
Router(config-if)# switchport port-security mac-address 1000.2000.3000
Router(config-if)#
```

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

```
Router(config-if)# no switchport port-security mac-address 1000.2000.3000
Router(config-if)#
```

This example shows how to enable the sticky feature on an interface:

```
Router(config-if)# switchport port-security mac-address sticky
Router(config-if)#
```

This example shows how to disable the sticky feature on an interface:

```
Router(config-if)# no switchport port-security mac-address sticky
Router(config-if)#
```

This example shows how to make a specific MAC address as a sticky address:

```
Router(config-if)# switchport port-security mac-address sticky 0000.0000.0001
Router(config-if)#
```

This example shows how to delete a specific sticky address:

```
Router(config-if)# no switchport port-security mac-address sticky 0000.0000.0001
Router(config-if)#
```

This example shows how to delete all sticky and static addresses that are configured on an interface:

```
Router(config-if)# no switchport port-security mac-address
Router(config-if)#
```

**Related Commands**

Command	Description
<a href="#">show port-security</a>	Displays information about the port-security setting.
<a href="#">clear port-security</a>	Deletes configured secure MAC addresses and sticky MAC addresses from the MAC-address table.

# switchport port-security maximum

To set the maximum number of secure MAC addresses on a port, use the **switchport port-security maximum** command. To return to the default settings, use the **no** form of this command.

**switchport port-security maximum** *maximum* [**vlan** *vlan* | *vlan-list*]

**no switchport port-security maximum**

Syntax Description	<i>maximum</i>	Maximum number of secure MAC addresses for the interface; valid values are from 1 to 4097.
	<b>vlan</b> <i>vlan</i>   <i>vlan-list</i>	(Optional) Specifies a VLAN or range of VLANs; see the “Usage Guidelines” section for additional information.

Defaults *vlan* is 1.

Command Modes Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** If you enter this command more than once, subsequent use of this command overrides the previous value of *maximum*. If the new *maximum* argument is larger than the current number of the secured addresses on this port, there is no effect except to increase the value of the *maximum*.

If the new *maximum* is smaller than the old *maximum* and there are more secure addresses on the old *maximum*, the command is rejected.

If you configure fewer secure MAC addresses than the maximum number of secure MAC addresses on the port, the remaining MAC addresses are dynamically learned.

Once the maximum number of secure MAC addresses for the port is reached, no more addresses are learned on that port even if the per-VLAN port maximum is different from the aggregate maximum number.

You can override the maximum number of secure MAC addresses for the port for a specific VLAN or VLANs by entering the **switchport port-security maximum** *maximum* **vlan** *vlan* / *vlan-list* command.

The *vlan-list* argument allows you to enter ranges, commas, and delimited entries such as 1,7,9-15,17.

The *vlan-list* argument is visible only if the port has been configured and is operational as a trunk. Enter the **switchport mode trunk** command and then enter the **switchport nonegotiate** command.

**Examples** This example shows how to set the maximum number of secure MAC addresses that are allowed on this port:

```
Router(config-if)# switchport port-security maximum 5
```

```
Router(config-if)#
```

This command shows how to override the maximum set for a specific VLAN:

```
Router(config-if)# switchport port-security maximum 3 vlan 102  
Router(config-if)#
```

---

**Related Commands**

Command	Description
<a href="#">show port-security</a>	Displays information about the port-security setting.

---

# switchport port-security violation

To set the action to be taken when a security violation is detected, use the **switchport port-security violation** command. To return to the default settings, use the **no** form of this command.

**switchport port-security violation { shutdown | restrict | protect }**

Syntax Description	shutdown	restrict	protect
	Shuts down the port if there is a security violation.	Drops all the packets from the insecure hosts at the port-security process level and increments the security-violation count.	Drops all the packets from the insecure hosts at the port-security process level but does not increment the security-violation count.

**Defaults** shutdown

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

Port-security violations occur because of the following reasons:

- If the number of source MAC addresses seen on an interface is more than the port-security limit.
- If a source MAC address secured on one port appears on another secure port. The violation occurs in this situation because in restrict/protect mode the software is hit by the violation traffic. The software can be protected from this condition by using **mls rate-limit layer2 port-security** command.

When a security violation is detected, one of the following actions occurs:

- **Protect**—When the number of port-secure MAC addresses reaches the maximum limit that is allowed on the port, the packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses.
- **Restrict**—A port-security violation restricts data and causes the security-violation counter to increment.
- **Shutdown**—The interface is error disabled when a security violation occurs.



### Note

When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause psecure-violation** global configuration command or you can manually reenble it by entering the **shutdown** and **no shutdown** commands in interface-configuration mode.

---

**Examples**

This example shows how to set the action to be taken when a security violation is detected:

```
Router(config-if)# switchport port-security violation restrict
Router(config-if)#
```

---

**Related Commands**

Command	Description
<a href="#">show port-security</a>	Displays information about the port-security setting.

---

# 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

<i>primary-vlan-id</i>	Number of the primary VLAN of the PVLAN relationship; valid values are from 1 to 4094.
<i>secondary-vlan-id</i>	Number of the secondary VLAN of the private VLAN relationship; valid values are from 1 to 4094.

## Defaults

No PVLAN is configured.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

There is no run-time effect on the port unless it is in PVLAN-host mode. If the port is in PVLAN-host mode but neither of the VLANs exist, the command is allowed but the port is made inactive.

The secondary VLAN may be an isolated or community VLAN.

## Examples

This example shows how to configure a port with a primary VLAN (VLAN 18) and secondary VLAN (VLAN 20):

```
Router(config-if)# switchport private-vlan host-association 18 20
Router(config-if)#
```

This example shows how to remove the PVLAN association from the port:

```
Router(config-if)# no switchport private-vlan host-association
Router(config-if)#
```

## Related Commands

Command	Description
<a href="#">show interfaces switchport</a>	Displays the administrative and operational status of a switching (nonrouting) port.
<a href="#">switchport mode</a>	Sets the interface type for this command.

# switchport private-vlan mapping

To define the PVLAN mapping for a promiscuous port, use the **switchport private-vlan mapping** command. To clear all mappings from the primary VLAN, use the **no** form of this command.

```
switchport private-vlan mapping {primary-vlan-id} {secondary-vlan-list} |
  {add secondary-vlan-list} | {remove secondary-vlan-list}
```

```
no switchport private-vlan mapping
```

Syntax Description	
<i>primary-vlan-id</i>	Number of the primary VLAN of the PVLAN relationship; valid values are from 1 to 4094.
<i>secondary-vlan-id</i>	Number of the secondary VLAN of the private VLAN relationship; valid values are from 1 to 4094.
<b>add</b>	Maps the secondary VLANs to the primary VLAN.
<b>remove</b>	Clears mapping between the secondary VLANs and the primary VLAN.

**Defaults** No PVLAN mappings are configured.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** There is no run-time effect on the port unless it is in PVLAN-promiscuous mode. If the port is in PVLAN-promiscuous mode but the VLANs do not exist, the command is allowed but the port is made inactive.

The secondary VLAN may be an isolated or community VLAN.

**Examples** This example shows how to configure the mapping of primary VLAN 18 to secondary isolated VLAN 20 on a port:

```
Router(config-if)# switchport private-vlan mapping 18 20
Router(config-if)#
```

This example shows how to add a VLAN to the mapping:

```
Router(config-if)# switchport private-vlan mapping 18 add 21
Router(config-if)#
```

This example shows how to remove the PVLAN mapping from the port:

```
Router(config-if)# no switchport private-vlan mapping
Router(config-if)#
```

■ switchport private-vlan mapping

Related Commands	Command	Description
	<a href="#">show interfaces private-vlan mapping</a>	Displays the information about the PVLAN mapping for VLAN SVIs.

# switchport trunk

To set the trunk characteristics when the interface is in trunking mode, use the **switchport trunk** command. To reset all of the trunking characteristics back to the default settings, use the **no** form of this command.

**switchport trunk encapsulation** {isl | {dot1q [ethertype value]} | negotiate}

**switchport trunk native vlan** *vlan-id*

**switchport trunk allowed vlan** *vlan-list*

**switchport trunk pruning vlan** *vlan-list*

**no switchport trunk** {encapsulation {isl | dot1q | negotiate}} | {native vlan} | {allowed vlan} | {pruning vlan}

Syntax Description	
<b>encapsulation isl</b>	Sets the trunk-encapsulation format to ISL.
<b>encapsulation dot1q</b>	Sets the switch port-encapsulation format to 802.1Q.
<b>ethertype value</b>	Sets the EtherType value; valid values are from 0x0 to 0x5EF-0xFFFF.
<b>encapsulation negotiate</b>	Specifies that if DISL and DTP negotiations do not resolve the encapsulation format, then ISL is the selected format.
<b>native vlan</b> <i>vlan-id</i>	Sets the native VLAN for the trunk in 802.1Q trunking mode; valid values are from 1 to 4094.
<b>allowed vlan</b> <i>vlan-list</i>	Allowed VLANs that transmit this interface in tagged format when in trunking mode; valid values are from 1 to 4094.
<b>pruning vlan</b> <i>vlan-list</i>	List of VLANs that are enabled for VTP pruning when in trunking mode; valid values are from 1 to 4094.

## Defaults

The defaults are as follows:

- The encapsulation type is dependent on the platform or interface hardware.
- The access VLAN and trunk-interface native VLAN are default VLANs that correspond to the platform or interface hardware.
- All VLAN lists include all VLANs.
- **ethertype value** for 802.1Q encapsulation is 0x8100.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

This command is not supported on GE Layer 2 WAN ports.

The **switchport trunk encapsulation** command is supported only for platforms and interface hardware that can support both ISL and 802.1Q formats.

If you enter the **switchport trunk encapsulation isl** command on a port channel containing an interface that does not support ISL-trunk encapsulation, the command is rejected.

You can enter the **switchport trunk allowed vlan** command on interfaces where the span destination port is either a trunk or an access port.



## Note

The **switchport trunk pruning vlan** *vlan-list* command does not support extended-range VLANs; valid *vlan-list* values are from 1 to 1005.

The **dot1q ethertype** *value* keyword and argument are not supported on port-channel interfaces. You can enter the command on the individual port interface only. Also, you can configure the ports in a channel group to have different EtherType configurations.



## Caution

Be careful when configuring the custom EtherType value on a port. If you enter the **negotiate** keywords and DISL and DTP negotiation do not resolve the encapsulation format, then ISL is the selected format and may pose as a security risk. The **no** form of this command resets the trunk-encapsulation format back to the default.

The **no** form of the **native vlan** command resets the native mode VLAN to the appropriate default VLAN for the device.

The **no** form of the **allowed vlan** command resets the list to the default list, which allows all VLANs.

The **no** form of the **pruning vlan** command resets the list to the default list, which enables all VLANs for VTP pruning.

The **no** form of the **dot1q ethertype** *value* command resets the list to the default value.

The *vlan-list* format is **all** | **none** | **add** | **remove** | **except** *vlan-list*[,*vlan-list*...] and is described as follows:

- **all** specifies all the appropriate VLANs. This keyword is not supported in the **switchport trunk pruning vlan** command.
- **none** indicates an empty list. This keyword is not supported in the **switchport trunk allowed vlan** command.
- **add** adds the defined list of VLANs to those currently set instead of replacing the list.
- **remove** removes the defined list of VLANs from those currently set instead of replacing the list. You can remove VLAN 1. If you remove VLAN 1 from a trunk, the trunk interface continues to send and receive management traffic (for example, CDP3, VTP, PAgP4, and DTP) in VLAN 1.



## Note

You can remove any of the default VLANs (1002 to 1005) from a trunk; this action is not allowed in earlier releases.

- **except** lists the VLANs that should be calculated by inverting the defined list of VLANs.
- *vlan-list* is either a single VLAN number from 1 to 4094 or a continuous range of VLANs that are described by two VLAN numbers. The smaller number is first, separated by a hyphen that represents the VLAN IDs of the allowed VLANs when this port is in trunking mode.

Do not enable the reserved VLAN range (1006 to 1024) on trunks when connecting a Catalyst 6500 series switch running the Cisco IOS software on both the supervisor engine and the PISA to a Catalyst 6500 series switch running the Catalyst operating system. These VLANs are reserved in Catalyst 6500 series switches running the Catalyst operating system. If enabled, Catalyst 6500 series switches running the Catalyst operating system may error disable the ports if there is a trunking channel between these systems.

### 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:

```
Router(config-if)# switchport trunk encapsulation dot1q
Router(config-if)#
```

### Related Commands

Command	Description
<a href="#">show interfaces switchport</a>	Displays the administrative and operational status of a switching (nonrouting) port.

## switchport vlan mapping

To map the traffic arriving on the VLAN *original-vlan-id* to the VLAN *translated-vlan-id* and the traffic that is internally tagged with the VLAN *translated-vlan-id* with the VLAN *original-vlan-id* before leaving the port, use the **switchport vlan mapping** command. To clear the mapping between a pair of VLANs or clear all the mappings that are configured on the switch port, use the **no** form of this command.

**switchport vlan mapping** *original-vlan-id translated-vlan-id*

**no switchport vlan mapping** { *original-vlan-id translated-vlan-id* | **all** }

Syntax Description		
	<i>original-vlan-id</i>	Original VLAN number; valid values are from 1 to 4094.
	<i>translated-vlan-id</i>	Translated VLAN number; valid values are from 1 to 4094.
	<b>all</b>	Clears all the mappings that are configured on the switch port.

**Defaults** No mappings are configured on any switch port.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command is not supported on GE Layer 2 WAN ports.

You must enable VLAN translation on the port where you want VLAN translation to work. Use the **switchport vlan mapping enable** command to enable VLAN translation.

Do not remove the VLAN that you are translating from the trunk. When you map VLANs, make sure that both VLANs are allowed on the trunk that carries the traffic.

[Table 2-95](#) lists the VLAN translation, the type of VLAN translation support, the number of ports that you can configure per port group, and the trunk type for each module that supports VLAN translation.

**Table 2-95 Modules that Support VLAN Translation**

Product Number	VLAN Translation Support Type	Number of Port Groups	Port Ranges per Port Group	Translations per Port Group	VLAN Translation Trunk-Type Support
WS-SUP720	Per port group	1	1-2	32	802.1Q
WS-X6501-10GEX4	Per port	1	1 port in 1 group	32	802.1Q
WS-X6502-10GE	Per port	1	1 port in 1 group	32	802.1Q
WS-X6516A-GBIC	Per port group	2	1-8, 9-16	32	802.1Q
WS-X6516-GBIC	Per port group	2	1-8, 9-16	32	802.1Q
WS-X6516-GE-TX	Per port group	2	1-8, 9-16	32	802.1Q

Table 2-95 Modules that Support VLAN Translation (continued)

Product Number	VLAN Translation Support Type	Number of Port Groups	Port Ranges per Port Group	Translations per Port Group	VLAN Translation Trunk-Type Support
WS-X6524-100FX-MM	Per port group	1	1-24	32	ISL and 802.1Q
WS-X6548-RJ-45	Per port group	1	1-48	32	ISL and 802.1Q
WS-X6548-RJ-21	Per port group	1	1-48	32	ISL and 802.1Q

The mapping that you configured using the **switchport vlan mapping** command does not become effective until the switch port becomes an operational trunk port.

The VLAN mapping that is configured on a port may apply to all the other ports on the same ASIC. In some cases, a mapping that is configured on one of the ports on an ASIC can overwrite a mapping that is already configured on another port on the same ASIC.

The port VLAN mapping is applied to all the ports on a port ASIC if that ASIC does not support per-port VLAN mapping.

If you configure VLAN mapping on the port ASIC that is a router port, the port-VLAN mapping does not take effect until the port becomes a switch port.

You can map any two VLANs regardless of the trunk types carrying the VLANs.

### Examples

This example shows how to map the original VLAN to the translated VLAN:

```
Router(config-if)# switchport vlan mapping 100 201
Router(config-if)#
```

This example shows how to clear the mappings that are between a pair of VLANs:

```
Router(config-if)# no switchport vlan mapping 100 201
Router(config-if)#
```

This example shows how to clear all the mappings that are configured on the switch port:

```
Router(config-if)# no switchport vlan mapping 100 201
Router(config-if)#
```

Related Commands	Command	Description
	<a href="#">show interfaces vlan mapping</a>	Displays the status of a VLAN mapping on a port.
	<a href="#">show vlan mapping</a>	Registers a mapping of an 802.1Q VLAN to an ISL VLAN.
	<a href="#">switchport vlan mapping enable</a>	Enables VLAN mapping per switch port.

# switchport vlan mapping enable

To enable VLAN mapping per switch port, use the **switchport vlan mapping enable** command. To disable VLAN mapping per switch port, use the **no** form of this command.

**switchport vlan mapping enable**

**no switchport vlan mapping enable**

## Defaults

VLAN mapping is disabled on all switch ports.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines



### Note

You must enter the **switchport vlan mapping enable** command on the port where you want the mapping to take place.

See [Table 2-95](#) for a list of modules that support this command.

The **switchport vlan mapping enable** command enables or disables VLAN-mapping lookup in the hardware regardless of whether the mapping is configured by the global VLAN mapping command or the switchport VLAN mapping command.

This command is useful on the hardware that supports VLAN mapping per ASIC only because you can turn on or off VLAN translation selectively on ports that are connected to the same port ASIC.

## Examples

This example shows how to enable VLAN mapping per switch port:

```
Router(config-if)# switchport vlan mapping enable
Router(config-if)#
```

This example shows how to disable VLAN mapping per switch port:

```
Router(config-if)# no switchport vlan mapping enable
Router(config-if)#
```

■ switchport vlan mapping enable

Related Commands	Command	Description
	<a href="#">show interfaces vlan mapping</a>	Displays the status of a VLAN mapping on a port.
	<a href="#">show vlan mapping</a>	Registers a mapping of an 802.1Q VLAN to an ISL VLAN.
	<a href="#">switchport vlan mapping</a>	Maps the traffic arriving on the VLAN <i>original-vlan-id</i> to the VLAN <i>translated-vlan-id</i> and the traffic that is internally tagged with the VLAN <i>translated-vlan-id</i> with the VLAN <i>original-vlan-id</i> before leaving the port.

# switchport voice vlan

To configure a voice VLAN on a multiple-VLAN access port, use the **switchport voice vlan** command. To remove the voice VLAN from the switch port, use the **no** form of this command.

```
switchport voice vlan { dot1p | none | untagged | vvid }
```

```
no switchport voice vlan
```

Syntax Description		
	<b>dot1p</b>	Sends CDP packets that configure the IP phone to transmit voice traffic in the default VLAN in 802.1p frames that are tagged with a Layer 2 CoS value.
	<b>none</b>	Allows the IP phone to use its own configuration and transmit untagged voice traffic in the default VLAN.
	<b>untagged</b>	Sends CDP packets that configure the IP phone to transmit untagged voice traffic in the default VLAN.
	<i>vvid</i>	Voice VLAN identifier; valid values are from 1 to 4094. Sends CDP packets that configure the IP phone to transmit voice traffic in the voice VLAN in 802.1Q frames that are tagged with a Layer 2 CoS value.

Defaults	
	<b>none</b>

Command Modes	
	Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Usage Guidelines	
	The default Layer 2 CoS is 5. The default Layer 3 IP-precedence value is 5.
	This command does not create a voice VLAN. You can create a voice VLAN in VLAN-configuration mode by entering the <b>vlan (global configuration mode)</b> command. If you configure both the native VLAN and the voice VLAN in the VLAN database and set the switch port to multiple-VLAN access mode, this command brings up the switch port as operational.
	If you enter <b>dot1p</b> , the switch port is enabled to receive 802.1p packets only.
	If you enter <b>none</b> , the switch port does not send CDP packets with VVID TLVs.
	If you enter <b>untagged</b> , the switch port is enabled to receive untagged packets only.
	If you enter <i>vvid</i> , the switch port receives packets that are tagged with the specified <i>vvid</i> .

Examples	
	This example shows how to create an operational multiple-VLAN access port:

```
Router(config-if)# switchport  
Router(config-if)# switchport mode access
```

## ■ switchport voice vlan

```
Router(config-if)# switchport access vlan 100
Router(config-if)# switchport voice vlan 101
Router(config-if)
```

This example shows how to change the multiple-VLAN access port to a normal access port:

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# no switchport voice vlan
Router(config-if)
```

## Related Commands

Command	Description
<a href="#">switchport access vlan</a>	Sets the VLAN when the interface is in access mode.
<a href="#">switchport mode</a>	Sets the interface type.

# sync-restart-delay

To set the synchronization-restart delay timer to ensure accurate status reporting, use the **sync-restart-delay** command.

**sync-restart-delay** *timer*

<b>Syntax Description</b>	<i>timer</i>	Interval between status-register resets; valid values are from 200 to 60000 milliseconds.
---------------------------	--------------	---

<b>Defaults</b>	<i>timer</i> is <b>210</b> milliseconds.
-----------------	--

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

<b>Usage Guidelines</b>	This command is supported on Gigabit Ethernet fiber ports only. The status register records the current status of the link partner.
-------------------------	--

<b>Examples</b>	This example shows how to set the Gigabit Ethernet synchronization-restart delay timer: Router(config-if)# <b>sync-restart-delay 2000</b> Router(config-if)#
-----------------	--

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show running-config</a>	Displays the status and configuration of the module or Layer 2 VLAN.

# system flowcontrol bus

To set the FIFO overflow error count, use the **system flowcontrol bus** command. To return to the original FIFO threshold settings, use the **no** form of this command.

**[default] system flowcontrol bus {auto | on}**

**no system flowcontrol bus**

Syntax Description	default	(Optional) Specifies the default settings.
	<b>auto</b>	Monitors the FIFO overflow error count and sends a warning message if the FIFO overflow error count exceeds a configured error threshold in 5-second intervals.
	<b>on</b>	(Optional) Specifies the original FIFO threshold settings.

**Defaults** **auto**

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines



### Note

We recommend that you leave the system flow control in auto mode and use the other modes under the advice of Cisco TAC only.

## Examples

This example shows how to monitor the FIFO overflow error count and send a warning message if the FIFO overflow error count exceeds a configured error threshold in 5-second intervals:

```
Router(config)# system flowcontrol bus auto
Router(config)#
```

This example shows how to specify the original FIFO threshold settings:

```
Router(config)# system flowcontrol bus on
Router(config)#
```

# system jumbomtu

To set the maximum size of the Layer 2 and Layer 3 packets, use the **system jumbomtu** command. To revert to the default MTU setting, use the **no** form of this command.

**system jumbomtu** *mtu-size*

**no system jumbomtu**

<b>Syntax Description</b>	<i>mtu-size</i>	Maximum size of the Layer 2 and Layer 3 packets; valid values are from 1500 to 9216 bytes.
---------------------------	-----------------	--

<b>Defaults</b>	<i>mtu-size</i> is <b>9216</b> bytes.
-----------------	---------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** The *mtu-size* parameter specifies the Ethernet packet size, not the total Ethernet frame size. The Layer 3 MTU is changed as a result of entering the **system jumbomtu** command.

The **system jumbomtu** command enables the global MTU for port ASICs. On a port ASIC after jumbo frames are enabled, the port ASIC accepts any size packet on the ingress side and checks the outgoing packets on the egress side. The packets on the egress side that exceed the global MTU are dropped by the port ASIC.

For example, if you have port A in VLAN 1 and Port B in VLAN 2, and if VLAN 1 and VLAN 2 are configured for **mtu 9216** and you enter the **system jumbomtu 4000** command, the packets that are larger than 4000 bytes are not transmitted out because Ports B and A drop packets that are larger than 4000 bytes.

**Examples**

This example shows how to set the global MTU size to 1550 bytes:

```
Router(config)# system jumbomtu 1550
Router(config)# end
Router#
```

This example shows how to revert to the default MTU setting:

```
Router(config)# no system jumbomtu
Router(config)#
```

**Related Commands**

Command	Description
<a href="#">mtu</a>	Adjusts the maximum packet size or MTU size.
<a href="#">show interfaces</a>	Displays traffic that is seen by a specific interface.
<a href="#">show system jumbomtu</a>	Displays the global MTU setting.

# tcam priority

To prioritize the interfaces that are forwarded to the software in the event of TCAM entry or label exhaustion, use the **tcam priority** command.

**tcam priority { high | normal | low }**

Syntax Description	high	Sets priority to high.
	normal	Sets priority to normal.
	low	Sets priority to low.

Defaults	normal
----------	--------

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

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Usage Guidelines	<p>The interfaces are chosen in this order:</p> <ol style="list-style-type: none"> <li>1. Low-priority interfaces without VACLs and without multicast</li> <li>2. Low-priority interfaces without VACLs and approved by multicast</li> <li>3. Low-priority interfaces with VACLs and approved by multicast</li> <li>4. Low-priority interfaces (not approved by multicast)</li> <li>5. Normal-priority interfaces without VACLs and without multicast</li> <li>6. Normal-priority interfaces without VACLs and approved by multicast</li> <li>7. Normal-priority interfaces with VACLs and approved by multicast</li> <li>8. Normal-priority interfaces (not approved by multicast)</li> <li>9. High-priority interfaces without VACLs and without multicast</li> <li>10. High-priority interfaces without VACLs and approved by multicast</li> <li>11. High-priority interfaces with VACLs and approved by multicast</li> <li>12. High-priority interfaces (not approved by multicast)</li> </ol>
------------------	--

## ■ tcam priority

---

**Examples**

This example shows how to set the priority:

```
Router(config-if)# tcam priority low
Router(config-if)#
```

---

**Related Commands**

Command	Description
<a href="#">show tcam interface</a>	Displays information about the interface-based TCAM.

# test cable-diagnostics

To test the condition of 10-Gigabit Ethernet links or copper cables on 48-port 10/100/1000 BASE-T modules, use the **test cable-diagnostics** command.

**test cable-diagnostics tdr interface** {*interface interface-number*}

Syntax Description	tdr	Activates the TDR test for copper cables on 48-port 10/100/1000 BASE-T modules.
	<b>interface</b> <i>interface</i>	Specifies the interface type; see the “Usage Guidelines” section for valid values.
	<i>interface-number</i>	Module and port number.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Cable diagnostics can help you detect whether your cable has connectivity problems.

The TDR test guidelines are as follows:

- TDR can test cables up to a maximum length of 115 meters.
- See the Release Notes for Cisco IOS Release 12.2 ZY for the list of the modules that support TDR.
- The valid values for **interface** *interface* 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 up before running the TDR test. If the port is down, the **test cable-diagnostics tdr** command is rejected and the following message is displayed:
 

```
Router# test cable-diagnostics tdr interface gigabitethernet2/12
% Interface Gi5/45 is administratively down
% Use 'no shutdown' to enable interface before TDR test start1
```
- If the port speed is 1000 and the link is up, do not disable the auto-MDIX feature.
- For fixed 10/100 ports, before running the TDR test, disable auto-MDIX on both sides of the cable. Failure to do so can lead to misleading results.

- For all other conditions, you must disable the auto-MDIX feature on both ends of the cable (use the **no mdix auto** command). Failure to disable auto-MDIX will interfere with the TDR test and generate false results.
- If a link partner has auto-MDIX enabled, this action will interfere with the TDR-cable diagnostics test and test results will be misleading. The workaround is to disable auto-MDIX on the link partner.
- If you change the port speed from 1000 to 10/100, enter the **no mdix auto** command before running the TDR test. Note that entering the **speed 1000** command enables auto-MDIX regardless of whether the **no mdix auto** command has been run.

### Examples

This example shows how to run the TDR-cable diagnostics:

```
Router # test cable-diagnostics tdr interface gigabitethernet2/1
TDR test started on interface Gi5/4
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results1
Router #
```

### Related Commands

Command	Description
<b>clear cable-diagnostics tdr</b>	Clears a specific interface or clears all interfaces that support TDR.
<b>show cable-diagnostics tdr</b>	Displays the test results for the TDR cable diagnostics.

# time-range

To enable time-range configuration mode and define time ranges for functions (such as extended access lists), use the **time-range** command. To remove the time limitation, use the **no** form of this command.

**time-range** *time-range-name*

**no time-range** *time-range-name*

<b>Syntax Description</b>	<i>time-range-name</i> Name for the time range.				
<b>Defaults</b>	This command has no default settings.				
<b>Command Modes</b>	Global configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(18)ZY</td> <td>Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)ZY	Support for this command was introduced.
Release	Modification				
12.2(18)ZY	Support for this command was introduced.				
<b>Usage Guidelines</b>	<p>The <b>time-range</b> entries are identified by a name, which is referred to by one or more other configuration commands. Multiple time ranges can occur in a single access list or other feature.</p> <p>The <i>time-range-name</i> cannot contain a space or quotation mark and must begin with an alphabetical character.</p>				
 <b>Note</b>	<p>IP and IPX-extended access lists are the only types of access lists that can use time ranges.</p> <p>After you use the <b>time-range</b> command, use the <b>periodic</b> time-range configuration command, the <b>absolute</b> time-range configuration command, or some combination of those commands to define when the feature is in effect. Multiple <b>periodic</b> commands are allowed in a time range; only one <b>absolute</b> command is allowed.</p>				
 <b>Tips</b>	To avoid confusion, use different names for time ranges and named access lists.				

## Examples

This example shows how to deny HTTP traffic on Monday through Friday from 8:00 a.m. to 6:00 p.m. and allow UDP traffic on Saturday and Sunday from noon to midnight only:

```
Router(config)# time-range no-http
Router(config)# periodic weekdays 8:00 to 18:00
!
Router(config)# time-range udp-yes
Router(config)# periodic weekend 12:00 to 24:00
!
Router(config)# ip access-list extended strict
```

## time-range

```

Router(config)# deny tcp any any eq http time-range no-http
Router(config)# permit udp any any time-range udp-yes
!
Router(config)# interface ethernet 0
Router(config)# ip access-group strict in

```

## Related Commands

Command	Description
<b>absolute</b>	Specifies an absolute time when a time range is in effect.
<b>ip access-list</b>	Defines an IP access list by name.
<b>periodic</b>	Specifies a recurring (weekly) time range for functions that support the time-range feature.
<b>permit (IP)</b>	Sets conditions for a named IP access list.

# traceroute mac

To display the Layer 2 path taken by the packets from the specified source to the specified destination, use the **traceroute mac** command.

```
traceroute mac source-mac-address { destination-mac-address | { interface type interface-number
destination-mac-address } } [vlan vlan-id] [detail]
```

```
traceroute mac interface type interface-number source-mac-address { destination-mac-address |
{ interface type interface-number destination-mac-address } } [vlan vlan-id] [detail]
```

```
traceroute mac ip { source-ip-address | source-hostname } { destination-ip-address |
destination-hostname } [detail]
```

Syntax	Description
<i>source-mac-address</i>	MAC address of the source switch in hexadecimal format.
<i>destination-mac-address</i>	MAC address of the destination switch in hexadecimal format.
<b>interface</b> <i>type</i>	Specifies the interface where the MAC address resides; valid values are <b>FastEthernet</b> , <b>GigabitEthernet</b> , and <b>Port-channel</b> .
<i>interface-number</i>	Module and port number or the port-channel number; valid values for the port channel are from 1 to 282.
<b>vlan</b> <i>vlan-id</i>	(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 values are from 1 to 4094.
<b>detail</b>	(Optional) Displays detailed information about the Layer 2 trace.
<b>ip</b>	Specifies the IP address where the MAC address resides.
<i>source-ip-address</i>	IP address of the source switch as a 32-bit quantity in dotted-decimal format.
<i>source-hostname</i>	IP hostname of the source switch.
<i>destination-ip-address</i>	IP address of the destination switch as a 32-bit quantity in dotted-decimal format.
<i>destination-hostname</i>	IP hostname of the destination switch.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Do not use leading zeros when entering a VLAN ID.

You must enable CDP on all of the switches in the network. Do not disable CDP so that Layer 2 traceroute can function properly.

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 unicast traffic only. If you specify a multicast source or destination MAC address, the physical path is not identified, and a message appears.

The **tracert 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.

When multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port), the Layer 2 traceroute utility terminates at that hop and displays an error message.

This feature is not supported in Token Ring VLANs.

## Examples

This example shows how to display detailed information about the Layer 2 path:

```
Router# tracert mac 0001.0000.0204 0001.0000.0304 detail
Source 00041000010504 found on VA\U[WS-C6509] (51414140)
4 VA\U / WS-C6509 / 51414140 :
Gi6/4 [full, 4000M] => Po400 [auto, auto]
5 PANI / WS-C6509 / 51414145 :
Po400 [auto, auto] => Po440 [auto, auto]
3 BUMI / WS-C6509 / 51414143 :
Po440 [auto, auto] => Po450 [auto, auto]
4 AGNI / WS-C6509 / 51414144 :
Po450 [auto, auto] => Gi8/45 [full, 4000M]
Destination 00041000010304 found on AGNI[WS-C6509] (51414144)
Layer 5 trace completed1
Router#
```

This example shows the output when the switch is not connected to the source switch:

```
Router# tracert mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source 11111
Source 00001050410504 found on con5[WS-C6509] (5151515)
con5 / WS-C6509 / 5151515 :
Fa0/4 [auto, auto] =>Gi0/4 [auto, auto]
con4 / WS-C6509 / 5151414 :
Gi0/4 [auto, auto] =>Gi0/5 [auto, auto]
con5 / WS-C6509 / 5151515 :
Gi0/5 [auto, auto] =>Fa0/4 [auto, auto]
Destination 00001050410504 found on con5[WS-C6509] (5151515)
Layer 5 trace completed1
Router#
```

This example shows the output when the switch cannot find the destination port for the source MAC address:

```
Router# tracert mac 0000.0011.1111 0000.0201.0201
Error:Source Mac address not found1
Layer5 trace aborted1
Router#
```

This example shows the output when the source and destination devices are in different VLANs:

```
Router# tracert mac 0000.0201.0601 0000.0301.0201
```

```
Error:Source and destination macs are on different vlans1
Layer5 trace aborted1
Router#
```

This example shows the output when the destination MAC address is a multicast address:

```
Router# traceroute mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
Router#
```

This example shows the output when the source and destination switches belong to multiple VLANs:

```
Router# traceroute mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans1
Layer5 trace aborted1
Router#
```

This example shows how to display the Layer 2 path by specifying the interfaces on the source and destination switches:

```
Router# traceroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3 0000.0201.0201
Source 00001050410604 found on con6[WS-C6509] (5151616)
con6 (5151616) :Fa0/4 =>Fa0/3
con5          (5151515)   ) : Fa0/3 =>Gi0/4
con4          (5151414)   ) : Gi0/4 =>Gi0/5
con5          (5151515)   ) : Gi0/5 =>Fa0/4
Destination 00001050410504 found on con5[WS-C6509] (5151515)
Layer 5 trace completed
Router#
```

This example shows how to display detailed traceroute information:

```
Router# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac11111
515166166 =>00001050410604
515155155 =>00001050410504

Source 00001050410604 found on con6[WS-C6509] (5151616)
con6 / WS-C6509 / 5151616 :
      Fa0/4 [auto, auto] =>Fa0/3 [auto, auto]
con5 / WS-C6509 / 5151515 :
      Fa0/3 [auto, auto] =>Gi0/4 [auto, auto]
con4 / WS-C6509 / 5151414 :
      Gi0/4 [auto, auto] =>Gi0/5 [auto, auto]
con5 / WS-C6509 / 5151515 :
      Gi0/5 [auto, auto] =>Fa0/4 [auto, auto]
Destination 00001050410504 found on con5[WS-C6509] (5151515)
Layer 5 trace completed1
Router#
```

This example shows how to display the Layer 2 path by specifying the source and destination hostnames:

```
Router# traceroute mac ip con6 con2
Translating IP to mac 11111
515166166 =>00001050410604
515155155 =>00001050410504

Source 00001050410604 found on con6
con6 (5151616) :Fa0/4 =>Fa0/3
con5          (5151515)   ) : Fa0/3 =>Gi0/4
con4          (5151414)   ) : Gi0/4 =>Gi0/5
con5          (5151515)   ) : Gi0/5 =>Fa0/4
Destination 00001050410504 found on con5
Layer 5 trace completed
Router#
```

This example shows the output when ARP cannot associate the source IP address with the corresponding MAC address:

```
Router# traceroute mac ip 2.2.66.66 2.2.77.77  
Arp failed for destination 5151771771  
Layer5 trace aborted1  
Router#
```

# track interface

To configure an interface to be tracked and to enter tracking configuration mode, use the **track interface** command in global configuration mode. To remove the tracking, use the **no** form of this command.

**track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**}

**no track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**}

Syntax Description		
	<i>object-number</i>	Object number that represents the interface to be tracked; valid values are from 1 to 500.
	<i>type number</i>	Interface type and number to be tracked.
	<b>line-protocol</b>	Tracks the state of the interface line protocol.
	<b>ip routing</b>	Tracks if IP routing is enabled, if an IP address is configured on the interface, and if the interface state is up before reporting to the tracking client that the interface is up.

**Defaults** No interface is tracked.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** This command reports a state value to clients. A tracked IP-routing object is considered up when the following exists:

- IP routing is enabled and active on the interface.
- The interface line-protocol state is up.
- The interface IP address is known. The IP address is configured or received through the Dynamic Host Configuration Protocol (DHCP) or IP Control Protocol (IPCP) negotiation.

Interface IP routing will go down when one of the following exists:

- IP routing is disabled globally.
- The interface line-protocol state is down.
- The interface IP address is unknown. The IP address is not configured or received through DHCP or IPCP negotiation.

No space is required between the *type number* values.

Tracking the IP-routing state of an interface using the **track interface ip routing** command can be more useful in some situations than just tracking the line-protocol state using the **track interface line-protocol** command, especially on interfaces for which IP addresses are negotiated. For example, on a serial interface that uses the Point-to-Point Protocol (PPP), the line protocol could be up [link control protocol (LCP) negotiated successfully], but IP could be down (IPCP negotiation failed).

The **track interface ip routing** command supports the tracking of an interface with an IP address acquired through any of the following methods:

- Conventional IP address configuration
- PPP/IPCP
- DHCP
- Unnumbered interface

---

### Examples

This example shows how to configure the tracking process to track the IP-routing capability of serial interface 1/0:

```
Router(config)# track 1 interface serial1/0 ip routing
Router(config)#
```

---

### Related Commands

Command	Description
<b>show track</b>	Displays HSRP tracking information.

# transceiver type all monitoring

To enable monitoring on all transceivers, use the **transceiver type all monitoring** command. To disable monitoring, use the **no** form of this command.

**transceiver type all monitoring**

**no transceiver type all monitoring**

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

**Defaults** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** You can use the **transceiver type all monitoring** command to enable monitoring (for example, collecting DOM information and evaluating threshold violations) for all transceiver types.



**Note**

The **no transceiver type all monitoring** command overrides the **snmp-server enable traps transceiver type all** command and will not permit the generation of SNMP traps.

**Examples** This example shows how to enable monitoring for all transceiver types:

```
Router(config)# transceiver type all monitoring
Router(config)#
```

This example shows how to disable monitoring for all transceiver types:

```
Router(config)# no transceiver type all monitoring
Router(config)#
```

Related Commands	Command	Description
	<a href="#">snmp-server enable traps transceiver type all</a>	Enables all supported SNMP transceiver traps for all transceiver types.

## tunnel udldr address-resolution

To enable the forwarding of the ARP and NHRP over a UDL, use the **tunnel udldr address-resolution** command. To disable forwarding, use the **no** form of this command.

**tunnel udldr address-resolution**

**no tunnel udldr address-resolution**

---

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

---

**Defaults** Disabled

---

**Command Modes** Interface configuration

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Usage Guidelines** This command is supported on the following modules only:

- WS-X6704-10GE 4-port 10-Gigabit Ethernet
- WS-X6816-GBIC 16-port Gigabit Ethernet
- WS-X6516A-GBIC 16-port Gigabit Ethernet
- WS-X6516-GBIC 16-port Gigabit Ethernet

UDLR back-channel tunnels do not support IPv6.

This command is supported on the send-only tunnel interface of a downstream router only.

You cannot configure software-based UDE on non-physical interfaces.

An ARP address resolution request that is received from the upstream router on the UDL (Ethernet interface 0) is replied to over the send-only tunnel of the receiver. An ARP request may be sent by the downstream router over the send-only tunnel, and the response is received over the UDL.

---

**Examples** This example shows how to enable ARP and NHRP forwarding over a send-only tunnel:

```
Router(config-if)# tunnel udldr address-resolution
Router(config-if)#
```

---

**Related Commands**

Command	Description
<b>show ip igmp udlr</b>	Displays UDLR information for the connected multicast groups on the interfaces that have a UDL helper address configured.
<b>tunnel udlr receive-only</b>	Configures a unidirectional GRE tunnel to act as a back channel that can receive messages from an interface that is configured for unidirectional link routing.

## tunnel udlr receive-only

To configure a unidirectional GRE tunnel to act as a back channel that can receive messages from an interface that is configured for unidirectional link routing, use the **tunnel udlr receive-only** command. To remove the tunnel, use the **no** form of this command.

**tunnel udlr receive-only** *interface-type interface-number*

**no tunnel udlr receive-only** *interface-type interface-number*

<b>Syntax Description</b>	<i>interface-type</i> Interface type and number. <i>interface-number</i>
---------------------------	---

<b>Defaults</b>	No UDLR tunnel is configured.
-----------------	-------------------------------

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

<b>Command History</b>	<table border="1"> <thead> <tr> <th style="border-bottom: none;">Release</th> <th style="border-bottom: none;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border-top: none;">12.2(18)ZY</td> <td style="border-top: none;">Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)ZY	Support for this command was introduced.
Release	Modification				
12.2(18)ZY	Support for this command was introduced.				

<b>Usage Guidelines</b>	<p>This command is supported on the following modules only:</p>
-------------------------	---

- WS-X6704-10GE 4-port 10-Gigabit Ethernet
- WS-X6816-GBIC 16-port Gigabit Ethernet
- WS-X6516A-GBIC 16-port Gigabit Ethernet
- WS-X6516-GBIC 16-port Gigabit Ethernet

The UDLR back-channel tunnels do not support IPv6.

Use this command to configure a router that has a unidirectional interface with send-only capabilities. For example, you can use this command if you have traffic traveling through a satellite.

The *interface-type* and *interface-number* arguments must match the send-only interface type and number specified by the **interface** command.

The *interface-type* and *interface-number* arguments must match the unidirectional send-only interface type and number specified by the **interface** command. When the packets are received over the tunnel, the upper layer protocols treat the packets as if they are received over the unidirectional send-only interface.

You must configure the **tunnel udlr send-only** command at the opposite end of the tunnel.

For a description of the **ip igmp unidirectional-link** command, refer to the *Cisco IOS Release 12.2 Command Reference*.

**Examples**

This example shows how to configure a unidirectional GRE tunnel to act as a back channel that can receive messages from an interface that is configured for unidirectional link routing:

```
Router(config-if)# tunnel udlr receive-only serial 0
Router(config-if)#
```

**Related Commands**

Command	Description
<b>interface</b>	Selects an interface to configure and enters interface configuration mode.
<b>ip igmp unidirectional-link</b>	Configures an interface to be unidirectional and enables it for IGMP UDLR.
<b>show ip igmp udlr</b>	Displays UDLR information for the connected multicast groups on the interfaces that have a UDL helper address configured.
<b>tunnel udlr send-only</b>	Configures a unidirectional GRE tunnel to act as a back channel that can send messages from an interface that is configured for unidirectional link routing.

## tunnel udlr send-only

To configure a unidirectional GRE tunnel to act as a back channel that can send messages from an interface that is configured for unidirectional link routing, use the **tunnel udlr send-only** command. To remove the tunnel, use the **no** form of this command.

**tunnel udlr send-only** *interface-type interface-number*

**no tunnel udlr send-only** *interface-type interface-number*

### Syntax Description

<i>interface-type</i>	Interface type and number.
<i>interface-number</i>	

### Defaults

No UDLR tunnel is configured.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

This command is supported on the following modules only:

- WS-X6704-10GE 4-port 10-Gigabit Ethernet
- WS-X6816-GBIC 16-port Gigabit Ethernet
- WS-X6516A-GBIC 16-port Gigabit Ethernet
- WS-X6516-GBIC 16-port Gigabit Ethernet

The UDLR back-channel tunnels do not support IPv6.

Use this command to configure a router that has a unidirectional interface with receive-only capabilities. The UDLR tunnel will act as a back channel. For example, you can use this command if you have traffic traveling through a satellite.

The *interface-type* and *interface-number* arguments must match the unidirectional receive-only interface type and number specified by the **interface** command. When packets are sent by the upper layer protocols over the interface, they are redirected and sent over this GRE tunnel.

The *interface-type* and *interface-number* arguments must match the receive-only interface type and number specified by the **interface** command.

You must configure the **tunnel udlr receive-only** command at the opposite end of the tunnel.

**Examples**

This example shows how to configure a unidirectional GRE tunnel to act as a back channel that can send messages from an interface that is configured for unidirectional link routing:

```
Router(config-if)# tunnel udlr send-only serial 1
Router(config-if)#
```

**Related Commands**

Command	Description
<b>interface</b>	Selects an interface to configure and enters interface configuration mode.
<b>show ip igmp udlr</b>	Displays UDLR information for the connected multicast groups on the interfaces that have a UDL helper address configured.
<b>tunnel udlr address-resolution</b>	Enables the forwarding of the ARP and NHRP over a UDL.
<b>tunnel udlr receive-only</b>	Configures a unidirectional GRE tunnel to act as a back channel that can receive messages from an interface that is configured for unidirectional link routing.

# udld

To enable aggressive or normal mode in UDLD and set the configurable message time, use the **udld** command. To disable aggressive or normal mode in UDLD, use the **no** form of this command.

**udld { enable | aggressive }**

**no udld { enable | aggressive }**

**udld message time *message-timer-time***

**no udld message time**

Syntax Description	Command	Description
	<b>udld enable</b>	Enables UDLD in normal mode by default on all fiber interfaces.
	<b>udld aggressive</b>	Enables UDLD in aggressive mode by default on all fiber interfaces.
	<b>message time <i>message-timer-time</i></b>	Sets the period of time between UDLD probe messages on ports that are in advertisement mode and are currently determined to be bidirectional; valid values are from 7 to 90 seconds.

## Defaults

The defaults are as follows:

- UDLD is disabled on all fiber interfaces.
- *message-timer-time* is 15 seconds.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

Use the **no** form of this command to do the following:

- Disable normal-mode UDLD on all fiber ports by default.
- Disable aggressive-mode UDLD on all fiber ports by default.
- Disable the message timer.

If you enable aggressive mode, after all the neighbors of a port age out either in the advertisement or in the detection phase, UDLD restarts the linkup sequence to resynchronize with any potentially out-of-sync neighbor and shuts down the port if the message from the link is still undetermined.

This command affects fiber interfaces only. Use the **udld port** command in interface-configuration mode to enable UDLD on other interface types.

---

**Examples**

This example shows how to enable UDLD on all fiber interfaces:

```
Router (config)# udld enable
Router (config)#
```

---

**Related Commands**

Command	Description
<a href="#">show udld</a>	Displays the administrative and operational UDLD status.
<a href="#">udld port</a>	Enables UDLD on the interface or enables UDLD in aggressive mode on the interface.

# uddl port

To enable UDLD on the interface or enable UDLD in aggressive mode on the interface, use the **uddl port** command. To return to the default settings, use the **no** form of this command.

**uddl port [aggressive]**

**no uddl port [aggressive]**

## Syntax Description

**aggressive** (Optional) Enables UDLD in aggressive mode on this interface; see the “Usage Guidelines” section for additional information.

## Defaults

The defaults are as follows:

- Fiber interfaces are in the state of the global **uddl** (**enable** or **aggressive**) command.
- Nonfiber interfaces have UDLD disabled.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

This command does not appear in the CLI unless a GBIC is in the port that you are trying to enable.

Use the **uddl port** and **uddl port aggressive** commands on fiber ports to override the setting of the global **uddl** (**enable** or **aggressive**) command. Use the **no** form on fiber ports to remove this setting and return control of UDLD enabling back to the global **uddl** command, or in the case of nonfiber ports, to disable UDLD.

If you enable aggressive mode, after all the neighbors of a port age out either in the advertisement or in the detection phase, UDLD restarts the linkup sequence to resynchronize with any potentially out-of-sync neighbor and shuts down the port if the message from the link is still undetermined.

If the port changes from fiber to nonfiber or nonfiber to fiber, all configurations are maintained because the platform software detects a change of module or a GBIC change.

## Examples

This example shows how to cause any port interface to enable UDLD regardless of the current global **uddl** setting:

```
Router (config-if)# uddl port
Router (config-if)#
```

This example shows how to cause any port interface to enable UDLD in aggressive mode regardless of the current global **udld** (**enable** or **aggressive**) setting:

```
Router (config-if)# udld port aggressive
Router (config-if)#
```

This example shows how to cause a fiber port interface to disable UDLD regardless of the current global **udld** setting:

```
Router (config-if)# no udld port
Router (config-if)#
```

---

**Related Commands**

Command	Description
<b>show udld</b>	Displays the administrative and operational UDLD status.
<b>udld</b>	Enables aggressive or normal mode in UDLD and sets the configurable message time.

# udd reset

To reset all the ports that are shut down by UDLD and permit traffic to begin passing through them again (although other features, such as spanning tree, PAgP, and DTP, will behave normally if enabled), use the **udd reset** command.

## udd reset

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

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

**Command Modes** EXEC mode

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** If the interface configuration is still enabled for UDLD, these ports will begin to run UDLD again and may shut down for the same reason if the reason for the shutdown has not been corrected.

**Examples** This example shows how to reset all ports that are shut down by UDLD:

```
Router# udd reset
Router#
```

Related Commands	Command	Description
	<a href="#">show udd</a>	Displays the administrative and operational UDLD status.

# udp-port

To change the UDP port numbers to which a test sender sends test packets or a test receiver sends status reports, use the **udp-port** command. To remove the port numbers, use the **no** form of this command.

**udp-port** [**test-packet** *port-number*] [**status-report** *port-number*]

**no udp-port** [**test-packet** *port-number*] [**status-report** *port-number*]

## Syntax Description

<b>test-packet</b> <i>port-number</i>	(Optional) Specifies the UDP port number to which test packets are sent by a test sender.
<b>status-report</b> <i>port-number</i>	(Optional) Specifies the UDP port number to which status reports are sent by a test receiver.

## Defaults

The defaults are as follows:

- **test-packet** *port-number*—16384, the minimum value of an audio port
- **status-report** *port-number*—65535, the maximum value of a video port

## Command Modes

Manager configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

This command is supported on the following modules only:

- WS-X6704-10GE 4-port 10-Gigabit Ethernet
- WS-X6816-GBIC 16-port Gigabit Ethernet
- WS-X6516A-GBIC 16-port Gigabit Ethernet
- WS-X6516-GBIC 16-port Gigabit Ethernet

The **test-packet** *port-number* must be even if the packets are RTP encapsulated.

The **status-report** *port-number* must be odd if the packets are RTP encapsulated.

## Examples

This example shows how to change the UDP port number to which test packets are targeted to 20000:

```
Router(config-mrm-manager)# udp-port test-packet 20000
Router(config-mrm-manager)#
```

## Related Commands

Command	Description
<b>ip mrm</b>	Configures an interface to operate as a test sender or test receiver, or both, for MRM.

# undelete

To recover a file that is marked “deleted” on a flash file system, use the **undelete** command.

**undelete** *index* [*filesystem:*]

Syntax Description	
<i>index</i>	Number to index the file in the <b>dir</b> command output; valid values are from 1 to 1024.
<i>filesystem:</i>	(Optional) File system containing the file to undelete, followed by a colon; valid values are <b>bootflash:</b> , <b>disk0:</b> , <b>disk1:</b> , <b>flash:</b> , <b>slot0:</b> , or <b>sup-bootflash:</b> .

**Defaults** The default file system is specified when you enter the **cd** command.

**Command Modes** EXEC mode

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** On Class A flash file systems, when you delete a file, Cisco IOS software marks the file as deleted but does not erase the file. This command allows you to recover a deleted file on a specified flash-memory device. You must undelete a file by its index because you could have multiple deleted files with the same name. For example, the “deleted” list could contain multiple configuration files with the name router-config. You undelete by the index to indicate which of the many router-config files from the list to undelete. Use the **dir** command to learn the index number of the file that you want to undelete.

**bootflash:**, **flash:**, **disk0:**, **disk1:**, and **sup-bootflash:** are Class A file systems.

You cannot undelete a file if a valid (undeleted) file with the same name exists. Instead, you first delete the existing file and then undelete the file that you want. For example, if you had an undeleted version of the router-config file and you wanted to use a previous, deleted version instead, you could not simply undelete the previous version by index. You must first delete the existing router-config file and then undelete the previous router-config file by index. You can delete and undelete a file up to 15 times.

On Class A flash file systems, if you try to recover the configuration file that is pointed to by the CONFIG\_FILE environment variable, you are prompted to confirm recovery of the file. This prompt reminds you that the CONFIG\_FILE environment variable points to an undeleted file. To delete all files that are marked “deleted” on a flash-memory device permanently, use the **squeeze** command in EXEC mode.

**Examples** This example shows how to recover the deleted file whose index number is 1 to the flash PC card that is inserted in disk 0:

```
Router# undelete 1 disk0:
Router#
```

Related Commands	Command	Description
	<b>delete</b>	Deletes a file from a flash memory device or NVRAM.
	<b>dir</b>	Displays a list of files on a file system.
	<b>squeeze</b>	Deletes flash files permanently by squeezing a flash file system.

# unidirectional

To configure the software-based UDE, use the **unidirectional** command. To remove the software-based UDE configuration, use the **no** form of this command.

**unidirectional** { **send-only** | **receive-only** }

**no unidirectional**

Syntax Description	send-only	Specifies that the unidirectional transceiver transmits traffic only.
	receive-only	Specifies that the unidirectional transceiver receives traffic only.

**Defaults** UDE is disabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** UDE is supported on the interfaces of these switching modules:

- WS-X6704-10GE 4-port 10-Gigabit Ethernet
- WS-X6816-GBIC 16-port Gigabit Ethernet
- WS-X6516A-GBIC 16-port Gigabit Ethernet
- WS-X6516-GBIC 16-port Gigabit Ethernet

You do not need to configure software-based UDE on ports where you implement hardware-based UDE.

If an interface is configured with Unidirectional Ethernet or has a receive-only transceiver, UDLD is operationally disabled. Use the **show udld** command to display the configured and operational states of this interface.

When you apply the UDE configuration to an interface, the following warning message is displayed:

Warning!

```
Enable port unidirectional mode will automatically disable port udld1 \ou must manually ensure that the unidirectional link does not create a spanning tree loop in the network1
```

```
Enable 13 port unidirectional mode will automatically disable ip routing on the port1 \ou must manually configure static ip route and arp entry in order to route ip traffic1
```

**Examples** This example shows how to configure 10-Gigabit Ethernet port 1/1 as a UDE send-only port:

```
Router(config-if)# unidirectional send-only
```

Warning!

Enable port unidirectional mode will automatically disable port udld1 \ou must manually ensure that the unidirectional link does not create a spanning tree loop in the network1

Enable l3 port unidirectional mode will automatically disable ip routing on the port1 \ou must manually configure static ip route and arp entry in order to route ip traffic1  
Router(config-if)#

This example shows how to configure 10-Gigabit Ethernet port 1/2 as a UDE receive-only port:

```
Router(config-if)# unidirectional receive-only
```

Warning!

Enable port unidirectional mode will automatically disable port udld1 \ou must manually ensure that the unidirectional link does not create a spanning tree loop in the network1

Enable l3 port unidirectional mode will automatically disable ip routing on the port1 \ou must manually configure static ip route and arp entry in order to route ip traffic1  
Router(config-if)#

#### Related Commands

Command	Description
<a href="#">show interfaces status</a>	Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.
<a href="#">show interfaces unidirectional</a>	Displays the operational state of an interface with a receive-only transceiver.

# upgrade rom-monitor

To set the execution preference on a ROMMON, use the **upgrade rom-monitor** command.

```
upgrade rom-monitor {slot num} {sp | rp} {file filename}
```

```
upgrade rom-monitor {slot num} {sp | rp} {{invalidate | preference} {region1 | region2}}
```

## Syntax Description

<b>slot num</b>	Specifies the slot number of the ROMMON to be upgraded.
<b>sp</b>	Upgrades the ROMMON of the switch processor.
<b>rp</b>	Upgrades the ROMMON of the route processor.
<b>file filename</b>	Specifies the name of the SREC file; see the “Usage Guidelines” section for valid values.
<b>invalidate</b>	Invalidates the ROMMON of the selected region.
<b>preference</b>	Sets the execution preference on a ROMMON of the selected region.
<b>region1</b>	Selects the ROMMON in region 1.
<b>region2</b>	Selects the ROMMON in region 2.

## Defaults

This command has no default settings.

## Command Modes

Privileged EXEC mode

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines



### Caution

If you enter the **upgrade rom-monitor** command with no parameters, service may be interrupted.



### Caution

If you enter the **upgrade rom-monitor** command from a Telnet session instead of a console connection, service may be interrupted.

The **slot num** is required for this command to function properly.

The **sp** or **rp** keyword is required if you installed a supervisor engine in the specified slot.

Valid values for **file filename** include the following:

- **bootflash:**
- **disk0:**
- **disk1:**

---

**Examples**

This example shows how to upgrade the new ROMMON image to the flash device:

```
Router# upgrade rom-monitor slot 1 sp file tftp://dirt/tftpboot-users/A2_71059.srec
ROMMON image upgrade in progress
  Erasing flash
  Programming flash
  Verifying new image
ROMMON image upgrade complete
  The card must be reset for this to take effect
Router#
```

---

**Related Commands**

Command	Description
<a href="#">show rom-monitor</a>	Displays the ROMMON status.

## username secret

To establish a username-based authentication system, use the **username secret** command.

```
username name secret {0 | 5} password
```

Syntax Description	<i>name</i>	User ID.
	<b>secret 0   5</b>	Specifies the secret; valid values are <b>0</b> (text immediately following is not encrypted) and <b>5</b> (text immediately following is encrypted using an MD5-type encryption method).
	<i>password</i>	Password.

**Defaults** No username-based authentication system is established.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Use this command to enable Enhanced Password Security for the specified, un retrievable username. This command enables MD5 encryption on the password. MD5 encryption is a strong encryption method. You cannot use MD5 encryption with protocols, such as CHAP, that require clear-text passwords.

This command can be useful for defining usernames that get special treatment. For example, you can use this command to define an “info” username that does not require a password but connects the user to a general-purpose information service.

The **username secret** command provides a username and/or a secret authentication for login purposes only. The *name* argument can be one word only. White spaces and quotation marks are not allowed. You can use multiple **username secret** commands to specify options for a single user.

**Examples** This example shows how to configure a username xena and enter an MD5 encrypted text string that is stored as the username password:

```
Router(config)# username xena secret 5 $1$feb0$a104Qd9UZ./Ak00KTggPD0
Router(config)#
```

Related Commands	Command	Description
	<b>enable password</b>	Sets a local password to control access to various privilege levels.
	<b>enable secret</b>	Specifies an additional layer of security over the <b>enable password</b> command.

# verify

To verify the checksum of a file on a flash memory file system or compute an MD5 signature for a file, use the **verify** command.

```
verify {{{/md5 flash-filesystem} [expected-md5-signature]} | {/ios flash-filesystem} |
flash-filesystem}
```

Syntax Description		
<i>/md5 flash-filesystem</i>		Computes an MD5 signature for a file; valid values are <b>bootflash:</b> , <b>disk0:</b> , <b>disk1:</b> , <b>flash:</b> , or <b>sup-bootflash:</b> .
<i>expected-md5-signature</i>		(Optional) MD5 signature.
<i>/ios flash-filesystem</i>		Verifies the compressed Cisco IOS image checksum; valid values are <b>bootflash:</b> , <b>disk0:</b> , <b>disk1:</b> , <b>flash:</b> , or <b>sup-bootflash:</b> .
<i>flash-filesystem</i>		Device where the flash memory resides; valid values are <b>bootflash:</b> , <b>disk0:</b> , <b>disk1:</b> , <b>flash:</b> , or <b>sup-bootflash:</b> .

**Defaults** The default device is the current working device.

**Command Modes** Privileged EXEC mode

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** Each software image that is distributed on disk uses a single checksum for the entire image. This checksum is displayed only when the image is copied into the flash memory.

The Readme file, which is included with the image on the disk, lists the name, file size, and checksum of the image. Review the contents of the Readme file before loading or duplicating the new image so that you can verify the checksum when you copy it into the flash memory or onto a server.

Use the **verify /md5** command to verify the MD5 signature of a file before using it. This command validates the integrity of a copied file by comparing a precomputed MD5 signature with the signature that is computed by this command. If the two MD5 signatures match, the copied file is identical to the original file.

You can find the MD5 signature that is posted on the Cisco.com page with the image.



This example shows how to verify the compressed checksum of the Cisco IOS image:

```
Router# verify /ios disk0:c6k222-jsv-mz
Verified compressed IOS image checksum for disk0:c6k555-jsv-mz
Router#
```

---

**Related Commands**

Command	Description
<a href="#">copy /noverify</a>	Disables the automatic image verification for the current copy operation.
<a href="#">file verify auto</a>	Verifies the compressed Cisco IOS image checksum.
<a href="#">show file systems (flash file system)</a>	Lists available file systems.
<a href="#">show flash</a>	Displays the layout and contents of flash memory.

## vlan (config-VLAN submode)

To configure a specific VLAN, use the **vlan** command in config-VLAN submode. To delete a VLAN, use the **no** form of this command.

**vlan** *vlan-id*

**no vlan** *vlan*

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

### Defaults

The defaults are as follows:

- *vlan-name* is “VLANxxxx” where “xxxx” represents four numeric digits (including leading zeroes) equal to the VLAN ID number.
- **media type** is **ethernet**.
- **state** is **active**.
- *said-value* is 100000 plus the VLAN ID number.
- *mtu-size* default is dependent upon the VLAN type:
  - **ethernet**—1500
  - **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
- *ring-number* is that no ring number is specified.
- *bridge-number* is that no bridge number is specified.
- *parent-vlan-id* is that no parent VLAN is specified.
- *type* is that no STP type is specified.
- *tb-vlan1* and *tb-vlan2* is 0, which means that no translational-bridge VLAN is specified.

### Command Modes

config-VLAN submode

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

VLAN 1 parameters are factory configured and cannot be changed. You cannot delete VLAN 1.

Once you are in the config-VLAN submode, this syntax is available:

```
{are hops} {backupcrf mode} {bridge type | bridge-num} {exit} {media type} {mtu mtu-size}
{name vlan-name} {parent parent-vlan-id} {private-vlan} {remote-span} {ring
ring-number} {said said-value} {shutdown} {state {suspend | active}} {stp type type} {ste
hops} {tb-vlan1 tb-vlan1-id} {tb-vlan2 tb-vlan2-id}
```

```
no {are | backupcrf | {bridge type} | exit | media | mtu | name | parent | private-vlan |
remote-span | ring | said | shutdown | state | {stp type type} | {ste hops}}
```

<b>are hops</b>	Specifies the maximum number of All Route Explorer hops for this VLAN. Valid values are from 0 to 13; 0 is assumed if no value is specified.
<b>backupcrf mode</b>	Enables or disables the backup CRF mode of the VLAN; valid values are <b>enable</b> or <b>disable</b> .
<b>bridge type   bridge-num</b>	Specifies the bridging characteristics of the VLAN or identification number of the bridge; valid <i>type</i> values are <b>srb</b> or <b>srt</b> . Valid <i>bridge-num</i> values are from 0 to 15.
<b>exit</b>	Applies changes, increments the revision number, and exits config-VLAN submode.
<b>media type</b>	Specifies the media type of the VLAN; valid values are <b>ethernet</b> , <b>fd-net</b> , <b>fdi</b> , <b>trcrf</b> , and <b>trbrf</b> .
<b>mtu mtu-size</b>	Specifies the maximum transmission unit (packet size in bytes) that the VLAN can use; valid values are from 1500 to 18190.
<b>name vlan-name</b>	Defines a text string that is used as the name of the VLAN (1 to 32 characters).
<b>parent parent-vlan-id</b>	Specifies the ID number of the parent VLAN of FDDI or Token Ring-type VLANs; valid values are from 1 to 1005.
<b>private-vlan</b>	(Optional) Configures the VLAN as a PVLAN; see the <b>private-vlan</b> command.
<b>remote-span</b>	Configures the VLAN as an RSPAN VLAN.
<b>ring ring-number</b>	Specifies the ring number of FDDI or Token Ring-type VLANs; valid values are from 0 to 65535.
<b>said said-value</b>	Specifies the security-association identifier; valid values are from 1 to 4294967294.
<b>shutdown</b>	Shuts down VLAN switching.
<b>state {suspend   active}</b>	Specifies whether the state of the VLAN is active or suspended.
<b>stp type type</b>	Specifies the STP type; valid values are <b>ieee</b> , <b>ibm</b> , and <b>auto</b> .
<b>ste hops</b>	Specifies the maximum number of hops for Spanning Tree Explorer frames; valid values are from 0 to 13.
<b>tb-vlan1 tb-vlan1-id</b>	Specifies the ID number of the first translational VLAN for this VLAN. Valid values are from 1 to 1005; 0 is assumed if no value is specified.
<b>tb-vlan2 tb-vlan2-id</b>	Specifies the ID number of the second translational VLAN for this VLAN. Valid values are from 1 to 1005; 0 is assumed if no value is specified.

**Caution**

If you enter the **shutdown** command and then the **no shutdown** command in the config-vlan mode on a PVLAN (primary or secondary), the PVLAN type and association information is deleted. You will have to reconfigure the VLAN to be a PVLAN.

The VLANs in the suspended state do not pass packets.

The VLANs that are created or modified are not committed until you exit config-VLAN submode.

If you define *vlan-range* in global configuration mode, you are not allowed to set the *vlan-name* in config-vlan submode.

The maximum length of a Layer 2 VLAN name is 32 characters.

**Note**

If you attempt to add a new VLAN and the VLAN already exists, no action occurs.

For extended-range VLANs (1006 to 4094), only the **private-vlan**, **rspan**, and **mtu** VLAN parameters are configurable. The rest of the VLAN parameters for extended-range VLANs are set to default.

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 VLAN's 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 VLAN's source-routing bridge number returns to the default.

The parent VLAN resets to the default if the parent VLAN is deleted or the **media** keyword changes the VLAN type or the VLAN type of the parent VLAN.

The *tb-vlan1* and *tb-vlan2* are used to configure translational-bridge VLANs of a specified type of VLAN and are not allowed in other VLAN types. Translational-bridge VLANs must be different VLAN types than the affected VLAN; if two VLANs are specified, the two must be different VLAN types.

A translational-bridge VLAN resets to the default if you delete the translational-bridge VLAN or if you enter the **media** keyword to change the VLAN type or the VLAN type of the corresponding translational-bridge VLAN.

The **shutdown** keyword does not support extended-range VLANs.

To find out if a VLAN has been shut down internally, check the Status field in the **show vlan** command output. If a VLAN is shut down internally, these values appear in the Status field:

- act/ishut—VLAN status is active but shut down internally.
- sus/ishut—VLAN status is suspended but shut down internally.

**Examples**

This example shows how to add a new VLAN with all default parameters to the new VLAN database:

```
Router(config-vlan)# vlan 2
Router(config-vlan)#
```

This example shows how to cause the device to add a new VLAN, specify the media type and parent VLAN ID number 3, and set all other parameters to the defaults:

```
Router(config-vlan)# media ethernet parent 3
VLAN 5 modified:
  Media type ETHERNET
  Parent VLAN 3
Router(config-vlan)#
```

This example shows how to delete VLAN 2:

```
Router(config-vlan)# no vlan 2
Router(config-vlan)#
```

This example shows how to return to the default settings for the MTU for its type and translational-bridge VLANs:

```
Router(config-vlan)# no mtu tb-vlan1 tb-vlan2
Router(config-vlan)#
```

#### Related Commands

Command	Description
<a href="#">show vlan</a>	Displays VLAN information.

## vlan (global configuration mode)

To add a VLAN and enter config-VLAN submode, use the **vlan** command. To delete the VLAN, use the **no** form of this command.

**vlan** {*vlan-id* | *vlan-range*}

**no vlan** {*vlan-id* | *vlan-range*}

Syntax Description	<i>vlan-id</i>	Number of the VLAN; valid values are from 1 to 4094.
	<i>vlan-range</i>	Range of configured VLANs; see the “Usage Guidelines” section for a list of valid values.

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

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

VLAN 1 parameters are factory configured and cannot be changed.

The specified VLAN is added or modified in the VLAN database when you exit config-VLAN submode.

When you enter the **vlan** *vlan-id* command, a new VLAN is created with all default parameters in a temporary buffer and causes the CLI to enter config-VLAN submode. If the *vlan-id* that you entered matches an existing VLAN, nothing happens except that you enter config-VLAN submode.

If you define *vlan-range*, you are not allowed to set the *vlan-name* in config-VLAN submode.

You can enter the *vlan-range* using a comma (,), a dash (-), and the number.

See the **vlan (config-VLAN submode)** command for information on the commands that are available in the config-VLAN submode.

**Examples** This example shows how to add a new VLAN and enter config-VLAN submode:

```
Router (config)# vlan 2
Router (config-vlan)#
```

This example shows how to add a range of new VLANs and enter config-VLAN submode:

```
Router (config)# vlan 2,5,10-12,20,25,4000
Router (config-vlan)#
```

This example shows how to delete a VLAN:

```
Router (config)# no vlan 2
Router (config)#
```

---

**Related Commands**

Command	Description
<a href="#">vlan (config-VLAN submode)</a>	Configures a specific VLAN.

---

## vlan access-log

To configure the VACL-logging properties, including the log-table size, redirect-packet rate, and logging threshold, use the **vlan access-log** command. To return to the default settings, use the **no** form of this command.

```
vlan access-log { {maxflow max-number} | {ratelimit pps} | {threshold pkt-count}}
```

```
no vlan access-log { maxflow | ratelimit | threshold }
```

Syntax Description		
<b>maxflow</b> <i>max-number</i>	Specifies the maximum log-table size. Valid values are from 0 to 2048; 0 deletes the contents of the log table.	
<b>ratelimit</b> <i>pps</i>	Specifies the maximum redirect VACL-logging packet rate; valid values are from 0 to 5000.	
<b>threshold</b> <i>pkt-count</i>	Specifies the logging-update threshold; valid values are from 0 to 2147483647. 0 means that the threshold is not set.	

### Defaults

The defaults are as follows:

- *max-number* is **500**.
- *pps* is **2000** pps.
- *pkt-count* is not set.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

Due to the rate-limiting function for redirected packets, VACL-logging counters may not be accurate. Only denied IP packets are logged.

When the log-table size is full, the logging packets from the new flows are dropped by the software.

The packets that exceed the maximum redirect VACL-logging packet rate limit are dropped by the hardware.

A logging message is displayed if the flow threshold is reached before the 5-minute interval.

If you do not configure the maximum log-table size, maximum packet rate, or threshold, or if you enter the **no** form of the commands, the default values are assumed.

---

**Examples**

This example shows how to set the maximum log-table size:

```
Router(config)# vlan access-log maxflow 500
Router(config)#
```

This example shows how to set the maximum redirect VACL-logging packet rate after which packets are dropped:

```
Router(config)# vlan access-log ratelimit 200
Router(config)#
```

This example shows how to set the logging-update threshold:

```
Router(config)# vlan access-log threshold 3500
Router(config)#
```

---

**Related Commands**

Command	Description
<a href="#">show vlan access-log</a>	Displays information about the VACL logging including the configured logging properties.

## vlan access-map

To create a VLAN access map or enter VLAN access-map command mode, use the **vlan access-map** command. To remove a mapping sequence or the entire map, use the **no** form of this command.

**vlan access-map** *name* [*seq#*]

**no vlan access-map** *name* [*seq#*]

Syntax Description	<i>name</i>	VLAN access-map tag.
	<i>seq#</i>	(Optional) Map sequence number; valid values are 0 to 65535.

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

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

If you enter the sequence number of an existing map sequence, you enter VLAN access-map mode.

If you do not specify a sequence number, a number is automatically assigned. You can enter one match clause and one action clause per map sequence.

If you enter the **no vlan access-map name** [*seq#*] command without entering a sequence number, the whole map is removed.

Once you enter VLAN access-map mode, the following commands are available:

- **action**—Specifies the packet action clause; see the **action** command section.
- **default**—Sets a command to its defaults.
- **end**—Exits from configuration mode.
- **exit**—Exits from VLAN access-map configuration mode.
- **match**—Specifies the match clause; see the **match** command section.
- **no**—Negates a command or sets its defaults.

---

**Examples**

This example shows how to enter VLAN access-map mode:

```
Router(config)# vlan access-map Bob  
Router(config-access-map)#
```

---

**Related Commands**

Command	Description
<a href="#">action</a>	Sets the packet action clause.
<a href="#">match</a>	Specifies the match clause by selecting one or more ACLs for a VLAN access-map sequence.
<a href="#">show vlan access-map</a>	Displays the contents of a VLAN-access map.

# vlan database

To enter VLAN-configuration submode, 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
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** After you are in VLAN-configuration submode, you can access the **manipulation** commands in the VLAN-database editing buffer, including:

- **abort**—Exits mode without applying the changes.
- **apply**—Applies current changes and increments the revision number.
- **exit**—Applies changes, increments the revision number, and exits mode.
- **no**—Negates a command or sets its defaults; valid keywords are **vlan** and **vtp**.
- **reset**—Abandons current changes and releases the current database.
- **show**—Displays database information.
- **vlan**—Accesses subcommands to add, delete, or modify values that are associated with a single VLAN. For information about the **vlan** subcommands, see the [vlan \(config-VLAN submode\)](#) command.
- **vtp**—Accesses subcommands to perform VTP administrative functions. For information about the **vtp** subcommands, see the [vtp](#) command.

**Examples** This example shows how to enter VLAN-configuration mode:

```
Router# vlan database
Router(vlan)#
```

This example shows how to exit VLAN-configuration mode without applying changes after you are in VLAN-configuration mode:

```
Router(vlan)# abort
Aborting!!!!
Router#
```

This example shows how to delete a VLAN after you are in VLAN-configuration mode:

```
Router(vlan)# no vlan 100
Deleting VLAN 400111
Router(vlan)#
```

This example shows how to turn off pruning after you are in VLAN-configuration mode:

```
Router(vlan)# no vtp pruning
Pruning switched OFF
Router(vlan)#
```

---

**Related Commands**

Command	Description
<a href="#">show vlan</a>	Displays VLAN information.

---

## vlan dot1q tag native

To enable dot1q tagging for all VLANs in a trunk, use the **vlan dot1q tag native** command. To clear the configuration, use the **no** form of this command.

**vlan dot1q tag native**

**no vlan dot1q tag native**

---

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

---

**Defaults** Disabled

---

**Command Modes** Global configuration

---

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

---



---

**Usage Guidelines** The **vlan dot1q tag native** command configures the switch to tag native-VLAN traffic and admit only 802.1Q-tagged frames on 802.1Q trunks, dropping any untagged traffic, including untagged traffic in the native VLAN.

Follow these configuration guidelines when configuring Layer 2-protocol tunneling:

- On all the service-provider edge switches, you must enable spanning-tree BPDU filtering on the 802.1Q-tunnel ports by entering the **spanning-tree bpduguard enable** command.
- Ensure that at least one VLAN is available for native-VLAN tagging. If you use all the available VLANs and then enter the **vlan dot1q tag native** command, native-VLAN tagging is not enabled.
- On all the service-provider core switches, enter the **vlan dot1q tag native** command to tag native-VLAN egress traffic and drop untagged native-VLAN ingress traffic.
- On all the customer switches, either enable or disable native-VLAN tagging on each switch.




---

**Note** If you enable dot1q tagging on one switch and disable it on another switch, all traffic is dropped; you must identically configure dot1q tagging on each switch.

---

---

**Examples**

This example shows how to enable dot1q tagging for all VLANs in a trunk:

```
Router(config)# vlan dot1q tag native
Router(config)#
```

---

**Related Commands**

Command	Description
<a href="#">show vlan dot1q tag native</a>	Displays native VLAN-tagging information.

---

# 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* | **interface** *interface number* }

**no vlan filter** *map-name* { **vlan-list** [*vlan-list*] | **interface** [*interface interface-number*] }

Syntax Description	
<i>map-name</i>	VLAN access-map tag.
<i>vlan-list</i>	VLAN list; valid values are from 1 to 4094.
<b>interface</b> <i>interface</i>	Specifies the interface type; valid values are <b>pos</b> , <b>atm</b> , or <b>serial</b> . See the “Usage Guidelines” section for additional information.
<i>interface-number</i>	Interface number; see the “Usage Guidelines” section for additional information.

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

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

When configuring an action clause in a VLAN access map, note the following:

- You can apply the VLAN access map to one or more VLANs or WAN interfaces.
- The *vlan-list* argument can be a single VLAN ID, a list of VLAN IDs, or VLAN ID ranges (*vlan-id-vlan-id*). Multiple entries are separated by a hyphen (-) or a comma (,).
- If you delete a WAN interface that has a VACL applied, the VACL configuration on the interface is also removed.
- You can apply only one VLAN access map to each VLAN or WAN interface.
- VACLs that are applied to VLANs are active only for VLANs with a Layer 3-VLAN interface configured. VACLs that are applied to VLANs without a Layer 3-VLAN interface are inactive. Applying a VLAN access map to a VLAN without a Layer 3-VLAN interface creates an administratively down Layer 3-VLAN interface to support the VLAN access map. If creation of the Layer 3-VLAN interface fails, the VACL is inactive.

When entering the **no** form of this command, the *vlan-list* argument is optional (but the keyword **vlan-list** is required). If you do not enter the *vlan-list* argument, the VACL is removed from all VLANs where the *map-name* argument is applied.

When entering the **no** form of this command for WAN interfaces, the *interface* argument is optional (but the **interface** keyword is required). If you do not enter the *interface* argument, the VACL is removed from interfaces where the *map-name* is applied.

The **vlan filter** *map-name* **interface** command accepts only ATM, POS, or serial interface types. If your Catalyst 6500 series switch is not configured with any of these interface types, the **interface** *interface interface-number* keyword and argument are not provided.

The *interface-number* format can be *mod/port* or *slot/port-adapter/port*; it can include a subinterface or channel-group descriptor.

### Examples

This example shows how to apply a VLAN access map on VLANs 7 through 9:

```
Router(config)# vlan filter ganymede vlan-list 7-9
Router(config)#
```

### Related Commands

Command	Description
<a href="#">action</a>	Sets the packet action clause.
<a href="#">match</a>	Specifies the match clause by selecting one or more ACLs for a VLAN access-map sequence.
<a href="#">show vlan filter</a>	Displays information about the VLAN filter.

## vlan internal allocation policy

To configure the allocation direction of the internal VLAN, use the **vlan internal allocation policy** command. To return to the default settings, use the **no** form of this command.

**vlan internal allocation policy {ascending | descending}**

**no vlan internal allocation policy**

Syntax Description	
	<b>ascending</b> Allocates internal VLANs from 1006 to 4094.
	<b>descending</b> Allocates internal VLANs from 4094 to 1006.

Defaults	
	<b>ascending</b>

Command Modes	
	Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

Usage Guidelines	
	<p>You can configure internal VLAN allocation to be from 1006 and up or from 4094 and down.</p> <p>Internal VLANs and user-configured VLANs share the 1006 to 4094 VLAN spaces. A first in, first out (FIFO) policy is used in allocating these spaces.</p> <p>You must perform a system reboot before the <code>vlan internal allocation policy</code> command changes can take effect. During system bootup, internal VLANs that are required for features in the startup-config file are allocated first. The user-configured VLANs in the startup-config file are configured next. If you configure a VLAN that conflicts with an existing internal VLAN, the VLAN that you configured is put into a nonoperational status until the internal VLAN is freed and becomes available.</p> <p>After you enter the <b>write memory</b> command and the system reloads, the reconfigured allocation is used by the port manager.</p>

---

**Examples**

This example shows how to configure VLANs in a descending order as the internal VLAN-allocation policy:

```
Router(config)# vlan internal allocation policy descending  
Router(config)#
```

---

**Related Commands**

Command	Description
<a href="#">show vlan internal usage</a>	Displays information about the internal VLAN allocation.

## vlan mapping dot1q

To map an 802.1Q VLAN to an ISL VLAN, use the **vlan mapping dot1q** command. To remove a specified mapping or all 802.1Q VLAN-to-ISL VLAN mappings, use the **no** form of this command.

```
vlan mapping {dot1q dot1q-vlan-id} {isl isl-vlan-id}
```

```
no vlan mapping {dot1q dot1q-vlan-id | all}
```

Syntax Description	
<b>dot1q</b> <i>dot1q-vlan-id</i>	Specifies the VLAN ID of the 802.1Q VLAN from which the mapping occurs as traffic leaves and enters 802.1Q trunks on the local device; valid values are from 1 to 4094.
<b>isl</b> <i>isl-vlan-id</i>	Specifies the VLAN ID of the ISL VLAN onto which the mapping occurs as traffic leaves and enters 802.1Q trunks on the local device and specifies the VLAN ID of the 802.1Q VLAN for which to discard traffic as it arrives at a local device; valid values are from 1 to 4094.
<b>all</b>	Removes all 802.1Q VLAN-to-ISL VLAN mappings.

**Defaults** The default for 802.1Q VLAN IDs 1 to 4094 is an identity mapping.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines** VLAN 1 parameters are factory configured and cannot be changed.

You can map up to eight VLANs. You can map only one 802.1Q VLAN to an ISL VLAN. For example, if 802.1Q VLAN 800 has been automatically mapped to ISL VLAN 800, do not manually map any other 802.1Q VLANs to ISL VLAN 800.

You cannot overwrite existing 802.1Q-VLAN mapping. If the 802.1Q-VLAN number already exists, the command is aborted. You must first clear that mapping.

If the table is full, the command is aborted with an error message indicating that the table is full.

**Examples** This example shows how to map traffic arriving on 802.1Q trunks on VLAN 1001 to ISL VLAN 888 on the local device, discard traffic arriving on 802.1Q trunks on VLAN 888, and map traffic on ISL VLAN 888 on the local device to 802.1Q VLAN 1001 as it leaves the device:

```
Router(config)# vlan mapping dot1q 1001 isl 888
Router(config)#
```

This example shows how to clear the mapping of 802.1Q VLAN 1001 to ISL VLAN 888. The result is that 802.1Q VLAN 1001 traffic is discarded when it arrives on the local device, and 802.1Q VLAN 888 traffic is mapped to ISL VLAN 888 (both are their default states):

```
Router(config)# no vlan mapping dot1q 1001
No mapping for 4055
Router(config)#
```

**Related Commands**

Command	Description
<a href="#">show vlan</a>	Displays VLAN information.
<a href="#">vlan (config-VLAN submode)</a>	Configures a specific VLAN.
<a href="#">vlan database</a>	Enters VLAN-configuration submode.

# vtp

To configure the global VTP state, use the **vtp** command. To return to the default value.

```

vtp { domain domain-name }

vtp { file filename }

vtp { interface interface-name } [only]

vtp { mode { client | server | transparent } }

vtp { password password-value }

vtp pruning

vtp { version { 1 | 2 } }

```

Syntax	Description
<b>domain</b> <i>domain-name</i>	Sets the VTP-administrative domain name.
<b>file</b> <i>filename</i>	Sets the ASCII name of the IFS-file system file where the VTP configuration is stored.
<b>interface</b> <i>interface-name</i>	Sets the name of the preferred source for the VTP-updater ID for this device.
<b>only</b>	(Optional) Specifies to use only this interface's IP address as the VTP-IP updater address.
<b>mode client</b>	Sets the type of VTP-device mode to client mode.
<b>mode server</b>	Sets the type of VTP-device mode to server mode.
<b>mode transparent</b>	Sets the type of VTP-device mode to transparent mode.
<b>password</b> <i>password-value</i>	Specifies the administrative-domain password.
<b>pruning</b>	Enables the administrative domain to permit pruning.
<b>version 1   2</b>	Specifies the administrative-domain VTP-version number.

## Defaults

The defaults are as follows:

- **vtp domain** and **vtp interface** commands have no default settings.
- *filename* is **const-nvram:vlan.dat**.
- VTP mode is **mode server**.
- No password is configured.
- Pruning is disabled.
- **version 1**.

## Command Modes

Global configuration

**Command History**

Release	Modification
12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines****Note**

The **vtp pruning**, **vtp password**, and **vtp version** commands are also available in privileged EXEC mode. We recommend that you use these commands in global configuration mode only; do not use these commands in privileged EXEC mode.

Extended-range VLANs are not supported by VTP.

When you define the *domain-name*, the domain name is case sensitive and can be from 1 to 32 characters.

The *filename* and *interface-name* are ASCII strings from 1 to 255 characters.

You must configure a password on each network device in the management domain when the switch is in secure mode.

**Caution**

If you configure VTP in secure mode, the management domain does not function properly if you do not assign a management domain password to each network device in the domain.

A VTP version 2-capable network device can operate in the same VTP domain as a network device running VTP version 1 if VTP version 2 is disabled on the VTP version 2-capable network device (VTP version 2 is disabled by default).

Do not enable VTP version 2 on a network device unless all of the network devices in the same VTP domain are version 2 capable. When you enable VTP version 2 on a network device, all of the version 2-capable network devices in the domain enable VTP version 2.

In a Token Ring environment, you must enable VTP version 2 for VLAN switching to function properly.

Enabling or disabling VTP pruning on a VTP server enables or disables VTP pruning for the entire management domain.

Configuring VLANs as pruning eligible or pruning ineligible on a Catalyst 6500 series switch affects pruning eligibility for those VLANs on that switch only; it does not affect pruning eligibility on all network devices in the VTP domain.

The **vtp password**, **vtp pruning**, and **vtp version** commands are not placed in NVGEN but are included in the VTP transparent-mode startup configuration file.

Extended-range VLANs are not supported by VTP.

You can configure **pruning** in VTP-server mode; **version** is configurable in VTP-server mode or VTP transparent mode.

The *password-value* is an ASCII string from 8 to 64 characters identifying the administrative domain for the device.

VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if there are no stations belonging to that VLAN.

All Catalyst 6500 series switches in a VTP domain must run the same version of VTP. VTP version 1 and VTP version 2 do not operate on Catalyst 6500 series switches in the same VTP domain.

If all Catalyst 6500 series switches in a domain are VTP version 2 capable, you need to enable VTP version 2 on one Catalyst 6500 series switch; the version number is then propagated to the other version 2-capable Catalyst 6500 series switch in the VTP domain.

If you toggle the version 2 mode, certain default VLAN parameters are modified. See the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY* for additional information.

---

## Examples

This example shows how to set the device's management domain:

```
Router(config)# vtp domain DomainChandon
Router(config)#
```

This example shows how to specify the file in the IFS-file system where the VTP configuration is stored:

```
Router(config)# vtp file vtpconfig
Setting device to store VLAN database at filename vtpconfig1
Router(config)#
```

This example shows how to set the VTP mode to client:

```
Router(config)# vtp mode client
Setting device to VTP CLIENT model
Router(config)#
```

---

## Related Commands

Command	Description
<a href="#">show vtp</a>	Displays the VTP statistics and domain information.

## wrr-queue

To allocate the bandwidth between the standard transmit SRR, DWRR, or WRR queues, use the **wrr-queue** command. To return to the default settings, use the **no** form of this command.

```
wrr-queue [bandwidth | shape] { percent low-priority-queue-percentage
  [intermediate-priority-queue-percentages] high-priority-queue-percentage }
```

```
wrr-queue [bandwidth | shape] { percent low-priority-queue-weight
  [intermediate-priority-queue-weight] high-priority-queue-weight }
```

```
no wrr-queue [bandwidth | shape]
```

Syntax Description		
<b>bandwidth</b>	(Optional) Enters the <b>bandwidth</b> keyword to configure DWRR or WRR.	
<b>shape</b>	(Optional) Enters the <b>shape</b> keyword to configure SRR.	
<b>percent</b> <i>low-priority-queue-percentage</i>	(Optional) Specifies the minimum percentage; valid values are from 1 to 100.	
<i>intermediate-priority-queue-percentage</i>	(Optional) Intermediate percentage; valid values are from 1 to 100.	
<i>high-priority-queue-percentage</i>	Maximum percentage; valid values are from 1 to 100.	
<i>low-priority-queue-weight</i>	Minimum weight; valid values are from 1 to 255.	
<i>intermediate-priority-queue-weight</i>	(Optional) Intermediate weight; valid values are from 1 to 255.	
<i>high-priority-queue-weight</i>	Maximum weight; valid values are from 1 to 255.	

### Defaults

The defaults are listed in [Table 2-96](#).

**Table 2-96 Bandwidth Default Values**

Port Types	Default Value
2q8t	90:10
8q4t	90:0:0:0:0:0:10
8q8t	90:0:0:0:0:0:10
1p7q8t	22:33:45:0:0:0:0
1p2q1t	100:255
2q2t, 1p2q2t, and 1p2q1t	5:255
1p3q1t	100:150:255

### Command Modes

Interface configuration

**Command History**

Release	Modification
12.2(18)ZY	Support for this command was introduced.

**Usage Guidelines**

Shaped round robin (SRR) allows a queue to use only the allocated bandwidth. SRR is supported as an option on Supervisor Engine 32 SFP 1p3q8t ports and on 1p7q4t ports. Use of SRR prevents use of the strict priority queue. To configure SRR, any CoS or DSCP values mapped to a strict-priority queue must be remapped to a standard queue.

DWRR keeps track of any lower-priority queue under-transmission caused by traffic in a higher-priority queue and compensates in the next round. DWRR is the dequeuing algorithm on 1p3q1t, 1p2q1t, 1p3q8t, 1p7q4t, and 1p7q8t ports.

WRR allows a queue to use more than the allocated bandwidth if the other queues are not using any, up to the total bandwidth of the port. WRR is the dequeuing algorithm on all other ports.

The higher the percentage or weight that is assigned to a queue, the more transmit bandwidth is allocated to it. If you enter weights, the ratio of the weights divides the total bandwidth of the queue. For example, for three queues on a Gigabit Ethernet port, weights of 25:25:50 provide this division:

- Queue 1—250 Mbps
- Queue 2—250 Mbps
- Queue 3—500 Mbps

WRR allows bandwidth sharing at the egress port. This command defines the bandwidths for egress WRR through scheduling weights.

The WRR weights are used to partition the bandwidth between the queues if all queues are nonempty. For example, entering weights of 1:3 means that one queue gets 25 percent of the bandwidth and the other queue gets 75 percent.

Entering weights of 1:3 do not necessarily lead to the same results as entering weights at 10:30. Weights at 10:30 mean that more data is serviced from each queue and the latency of packets being serviced from the other queue goes up. You should set the weights so that at least one packet (maximum size) can be serviced from the lower priority queue at a time. For the higher priority queue, set the weights so that multiple packets are serviced at any one time.

Percentages should add up to 100. You must enter percentages for all the standard transmit queues on the port.

The valid values for weight range from 1 to 255. You must enter weights for all the standard transmit queues on the port.

**Examples**

This example shows how to allocate a three-to-one bandwidth ratio:

```
Router(config-if)# wrr-queue bandwidth 3 1
Router(config-if)#
```

**Related Commands**

Command	Description
<a href="#">show queueing interface</a>	Displays queueing information.
<a href="#">wrr-queue queue-limit</a>	Sets the transmit-queue size ratio on an interface.





## wrr-queue cos-map

To map CoS values to drop thresholds for a queue, use the **wrr-queue cos-map** command. To return to the default settings, use the **no** form of this command.

```
wrr-queue cos-map queue-id threshold-id cos-1 ... cos-n
```

```
no wrr-queue cos-map
```

Syntax Description	
<i>queue-id</i>	Queue number; the valid value is 1.
<i>threshold-id</i>	Threshold ID; valid values are from 1 to 4.
<i>cos-1</i> ... <i>cos-n</i>	CoS value; valid values are from 0 to 7.

### Defaults

The defaults are as follows:

- Receive queue 1/drop threshold 1 and transmit queue 1/drop threshold 1: CoS 0 and 1.
- Receive queue 1/drop threshold 2 and transmit queue 1/drop threshold 2: CoS 2 and 3.
- Receive queue 2/drop threshold 3 and transmit queue 2/drop threshold 1: CoS 4 and 6.
- Receive queue 2/drop threshold 4 and transmit queue 2/drop threshold 2: CoS 7.
- On 1p1q4t, 1p2q2t, and 1p3q1t interfaces, CoS 5 is mapped to the strict-priority queues.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

Enter up to eight CoS values to map to the threshold.

The threshold for 1p3q1t is always 1.

### Examples

This example shows how to map the CoS values 0 and 1 to standard transmit queue 1/threshold 1:

```
Router(config-if)# wrr-queue cos-map 1 1 0 1
Router(config-if)#
```

### Related Commands

<a href="#">show queueing interface</a>	Displays queueing information.
---	--------------------------------

## wrr-queue dscp-map

To map the hardware DSCP values to the drop threshold values for a queue, use the **wrr-queue dscp-map** command. To return to the default settings, use the **no** form of this command.

```
wrr-queue dscp-map queue-id threshold-id dscp-1 ... dscp-n
```

```
no wrr-queue dscp-map queue-id
```

Syntax Description	<i>queue-id</i>	Queue number; valid values are from 1 to 8.
	<i>threshold-id</i>	Threshold ID; valid values are from 1 to 4.
	<i>dscp-1 ... dscp-n</i>	DSCP value; valid values are from 0 to 7.

**Defaults** CoS mode

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines



#### Note

To enter the **wrr-queue dscp-map** command, the interface must be in DSCP-queuing mode. Use the **mls qos queue-mode mode-dscp** command to set the mode to DSCP.

This command is supported on 10-Gigabit Ethernet ports only.

When mapping DSCP values, follow these guidelines:

- You can enter up to eight DSCP values that map to a queue and threshold.
- You can enter multiple commands to map additional DSCP values to the queue and threshold.
- You must enter a separate command for each queue and threshold.

### Examples

This example shows how to map the hardware DSCP values to the drop threshold values for a queue:

```
Router(config-if)# wrr-queue dscp-map 8 1 0 1 2 3
Router(config-if)#
```

**Related Commands** [show queueing interface](#) Displays queueing information.

## wrr-queue queue-limit

To set the transmit-queue size ratio on an interface, use the **wrr-queue queue-limit** command. To return to the default settings, use the **no** form of this command.

```
wrr-queue queue-limit {queue1-weight [queue2-weight] queue3-weight}
```

```
no wrr-queue queue-limit
```

```
wrr-queue queue-limit {queue1-weight [queue2-weight] queue3-weight}
```

```
no wrr-queue queue-limit
```

Syntax Description		
<i>queue1-weight</i>	Ratio of the low-priority queue weight; valid values are from 1 and 100 percent.	
<i>queue2-weight</i>	(Optional) Ratio of the medium-priority queue weight; valid values are from 1 and 100 percent.	
<i>queue3-weight</i>	Ratio of the high-priority queue weight; see the “Usage Guidelines” section for valid values.	

### Defaults

The defaults are as follows:

- 90 percent for low priority
- 10 percent for high priority

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

Valid high-priority weight values are from 1 to 100 percent, except on 1p2q1t egress LAN ports, where valid values for the high-priority queue are from 5 to 100 percent.

On LAN ports that have an egress strict priority queue, PFC QoS sets the egress strict-priority queue size equal to the high-priority queue size.

Estimate the mix of low priority-to-high priority traffic on your network (for example, estimate 80 percent to low-priority traffic and 20 percent to high-priority traffic). Use the estimated percentages as queue weights.

Due to the granularity of programming the hardware, the values that are set in the hardware are close approximations of the provided values. For example, if you specify 0 percent, the actual value that is programmed is not necessarily 0.

---

**Examples**

This example shows how to configure the transmit-queue size ratio:

```
Router (config-if)# wrr-queue queue-limit 75 25
Router (config-if)#
```

---

**Related Commands**

Command	Description
<a href="#">show queueing interface</a>	Displays queueing information.
<a href="#">wrr-queue</a>	Allocates the bandwidth between the standard transmit queues.

## wrr-queue random-detect

To enable WRED or specify the minimum and maximum WRED threshold for the specified queues on 1p2q2t and 1p3q1t interfaces, use the **wrr-queue random-detect** command. To return to the default settings, use the **no** form of this command.

**wrr-queue random-detect** *queue-id*

**wrr-queue random-detect** { **max-threshold** | **min-threshold** } *queue-id* *threshold-percent-1* ...  
*threshold-percent-n*

**no wrr-queue random-detect** *queue-id*

**no wrr-queue random-detect** { **max-threshold** | **min-threshold** } *queue-id*

### Syntax Description

<i>queue-id</i>	Queue number; valid values are 1, 2, or 3.
<b>max-threshold</b>	Specifies the maximum WRED-drop threshold.
<b>min-threshold</b>	Specifies the minimum WRED-drop threshold.
<i>threshold-percent-1</i> <i>threshold-percent-n</i>	Threshold weights; valid values are from 1 to 100 percent.

### Defaults

The default is that WRED is disabled. When WRED is enabled, the defaults are as follows:

- The maximum threshold is (low) 40 percent and (high) 100 percent.
- The minimum thresholds are both set to zero.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

1p2q1t and 1p3q1t interfaces have WRED-drop thresholds in their standard transmit queues. You can configure 1p3q1t transmit queues to use a WRED-drop threshold or a tail-drop threshold.

To enable WRED-drop thresholds on 1p2p1t interfaces, enter the **wrr-queue random-detect** *queue-id* command. Use the **no** form of this command to disable WRED.

To enable WRED-drop thresholds on 1p3q1t interfaces, enter the **wrr-queue random-detect** *queue-id* command. To return to the tail-drop threshold, enter the **no wrr-queue random-detect** *queue-id* command.

The *queue-id* is 1 for the standard low-priority queue, 2 is for the standard high-priority queue, and 3 is for strict priority.

The threshold in the strict-priority queue is not configurable.

Each queue on a 1p2q2t interface has two thresholds; 1p3q1t interfaces have one threshold.

Each threshold has a low and a high WRED value.

WRED values are a percentage of the queue capacity.

For additional information on configuring WRED thresholds, refer to the QoS chapter in the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*.

### Examples

This example shows how to configure the low-priority transmit-queue high-WRED drop thresholds:

```
Router (config-if)# wrr-queue random-detect max-threshold 1 60 100
Router (config-if)#
```

### Related Commands

Command	Description
<a href="#">show queueing interface</a>	Displays queueing information.
<a href="#">wrr-queue queue-limit</a>	Sets the transmit-queue size ratio on an interface.

## wrr-queue shape

To configure the SRR maximum queue bandwidth with percentages or weights, use the **wrr-queue shape** command. To return to the default settings, use the **no** form of this command.

```
wrr-queue shape { percent low-priority-queue-percentage
  [intermediate-priority-queue-percentage] high-priority-queue-percentage }
```

```
wrr-queue shape { low-priority-queue-weight [intermediate-priority-queue-weight]
  high-priority-queue-weight }
```

```
no wrr-queue shape
```

Syntax Description		
<b>percent</b> <i>low-priority-queue-percentage</i>		Specifies the minimum SRR percentage; valid values are from 1 to 100.
<i>intermediate-priority-queue-percentage</i>		(Optional) Intermediate SRR percentage; valid values are from 1 to 100.
<i>high-priority-queue-percentage</i>		Maximum SRR percentage; valid values are from 1 to 100.
<i>low-priority-queue-weight</i>		Minimum SRR weight; valid values are from 1 to 255.
<i>intermediate-priority-queue-weight</i>		(Optional) Intermediate SRR weight; valid values are from 1 to 255.
<i>high-priority-queue-weight</i>		Maximum SRR weight; valid values are from 1 to 255.

### Defaults

The defaults are as follows:

- 1p3q8t—22:33:45
- 1p7q4t—100:150:200:0:0:0:0

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

### Usage Guidelines

SRR allows a queue to use only the allocated bandwidth.

This command is supported on SFP 1p3q8t ports and on 1p7q4t ports only.

You can configure up to seven queue weights.

Enter the **shape** keyword to configure SRR. If you use SRR, you cannot use the strict priority queue. To configure SRR, you must remap any CoS or DSCP values that are mapped to a strict-priority queue to a standard queue.

The higher the percentage or weight that is assigned to a queue, the more transmit bandwidth is allocated to it. If you enter weights, the ratio of the weights divides the total bandwidth of the queue. For example, for three queues on a Gigabit Ethernet port, weights of 25:25:50 provide this division:

- Queue 1—250 Mbps
- Queue 2—250 Mbps
- Queue 3—500 Mbps

Percentages should add up to 100. You must enter percentages for all the standard transmit queues on the port.

The valid values for weight range are from 1 to 255. You must enter weights for all the standard transmit queues on the port.

### Examples

This example shows how to allocate a three-to-one bandwidth ratio:

```
Router(config-if)# wrr-queue shape 3 1
Router(config-if)#
```

### Related Commands

Command	Description
<a href="#">show queueing interface</a>	Displays queueing information.
<a href="#">wrr-queue</a>	Allocates the bandwidth between the DWRR or WRR standard transmit queues.

# wrr-queue threshold

To configure the drop-threshold percentages for the standard receive and transmit queues on 1q4t and 2q2t interfaces, use the **wrr-queue threshold** command. To return to the default settings, use the **no** form of this command.

**wrr-queue threshold** *queue-id* *threshold-percent-1* ... *threshold-percent-n*

**no wrr-queue threshold** *queue-id*

## Syntax Description

<i>queue-id</i>	Queue number; valid values are 1 and 2.
<i>threshold-percent-1</i>	Number of weights for queues 1 and 2; valid values are from 1 to
<i>threshold-percent-n</i>	100 percent.

## Defaults

When you enable QoS, the default values are as follows:

- **100** percent for threshold 1
- **60** percent for threshold 2

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

## Usage Guidelines

Use the transmit queue and threshold numbers.

The *queue-id* is 1 for the standard low-priority queue and 2 for the standard high-priority queue.

Always set threshold 2 to 100 percent.

Receive-queue drop thresholds are supported only on Gigabit Ethernet interfaces that are configured to trust CoS.

## Examples

This example shows how to configure receive queue 1/threshold 1 and transmit queue 1/threshold 1:

```
Router(config-if)# wrr-queue threshold 1 60 100
Router(config-if)#
```

## Related Commands

Command	Description
<a href="#">show queueing interface</a>	Displays queueing information.
<a href="#">wrr-queue queue-limit</a>	Sets the transmit-queue size ratio on an interface.

■ wrr-queue threshold



## Acronyms

---

[Table A-1](#) defines the acronyms that are used in this publication.

**Table A-1** List of Acronyms

Acronym	Expansion
AAL	ATM adaptation layer
ACE	access control entry
ACL	access control list
ACNS	Application and Content Networking System
AFI	authority and format identifier
Agport	aggregation port
ALPS	Airline Protocol Support
AMP	Active Monitor Present
APaRT	Automated Packet Recognition and Translation
ARP	Address Resolution Protocol
ATA	Analog Telephone Adaptor or Advanced Technology Attachment
ATM	Asynchronous Transfer Mode
AV	attribute value
BDD	binary decision diagrams
BECN	backward explicit congestion notification
BGP	Border Gateway Protocol
Bidir-PIM	bidirectional PIM
BMA	broadcast multiaccess
BPDU	bridge protocol data unit
BRF	bridge relay function
BSC	Bisync
BSR	bootstrap router
BSTUN	Block Serial Tunnel
BUS	broadcast and unknown server
BVI	bridge-group virtual interface

**Table A-1 List of Acronyms (continued)**

<b>Acronym</b>	<b>Expansion</b>
CAM	content-addressable memory
CAR	committed access rate
CASA	Cisco Appliance Services Architecture
CBAC	context based access control
CCA	circuit card assembly
CDP	Cisco Discovery Protocol
CE	customer edge
CEF	Cisco Express Forwarding
CHAP	Challenge Handshake Authentication Protocol
CIR	committed information rate
CIST	Common and Internal Spanning Tree
CLI	command-line interface
CLNS	Connection-Less Network Service
CMM	Communication Media Module
CMNS	Connection-Mode Network Service
CNS	Cisco Networking Services
CoPP	control plane policing
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
CSM	Content Switching Module
CST	Common Spanning Tree
CUDD	University of Colorado Decision Diagram
CBWFQ	class-based weighted fair queueing
DAI	dynamic ARP inspection
DCC	Data Country Code
dCEF	distributed Cisco Express Forwarding
DDR	dial-on-demand routing
DE	discard eligibility
DEC	Digital Equipment Corporation
DF	designated forwarder
DFC	Distributed Forwarding Card
DFI	Domain-Specific Part Format Identifier

**Table A-1 List of Acronyms (continued)**

<b>Acronym</b>	<b>Expansion</b>
DFP	Dynamic Feedback Protocol
DHCP	Dynamic Host Configuration Protocol
DISL	Dynamic Inter-Switch Link
DLC	Data Link Control
DLCI	data-link connection identifier
DLSw	Data Link Switching
DMP	data movement processor
DNS	Domain Name System
DoD	Department of Defense
DOM	digital optical monitoring
DoS	denial of service
dot1q	802.1Q
dot1x	802.1x
DRAM	dynamic RAM
DRiP	Dual Ring Protocol
DSAP	destination service access point
DSCP	differentiated services code point
DSPU	downstream SNA Physical Units
DSS	Digital Signature Standard
DTP	Dynamic Trunking Protocol
DTR	data terminal ready
DVMRP	Distance Vector Multicast Routing Protocol
DWRR	deficit weighted round robin
DXI	data exchange interface
EAP	Extensible Authentication Protocol
EAPoUDP	Extensible Authentication Protocol over User Datagram 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
EOF	end of file
EoMPLS	Ethernet over Multiprotocol Label Switching
ERM	Exception Recovery Manager
ESI	end-system identifier

**Table A-1** *List of Acronyms (continued)*

<b>Acronym</b>	<b>Expansion</b>
FAT	File Allocation Table
FIB	Forwarding Information Base
FIE	Feature Interaction Engine
FECN	forward explicit congestion notification
FM	feature manager
FPD	field programmable devices
FRU	field replaceable unit
fsck	file system consistency check
FSM	feasible successor metrics
FSU	fast software upgrade
FTP	file transfer protocol
FWSM	Firewall Services Module
GARP	General Attribute Registration Protocol
GBIC	Gigabit Interface Converter
GBTE	guaranteed bandwidth traffic engineering
GE-WAN	Gigabit Ethernet WAN
GMRP	GARP Multicast Registration Protocol
GVRP	GARP VLAN Registration Protocol
HSRP	Hot Standby Routing Protocol
ICC	Inter-card Communication or interface controller card
ICD	International Code Designator
ICMP	Internet Control Message Protocol
IDB	interface descriptor block
IDP	initial domain part or Internet Datagram Protocol
IDS	Intrusion Detection System Module
IFS	IOS File System
IGMP	Internet Group Management Protocol
IGMPv2	IGMP version 2
IGMPv3	IGMP version 3
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol
ILMI	Integrated Local Management Interface
IP	Internet Protocol
IPC	interprocessor communication
IPG	inter packet gap
IPX	Internetwork Packet Exchange

**Table A-1 List of Acronyms (continued)**

<b>Acronym</b>	<b>Expansion</b>
IS-IS	Intermediate System-to-Intermediate System Intradomain Routing Protocol
ISL	Inter-Switch Link
ISL VLANs	Inter-Switch Link VLANs
ISO	International Organization of Standardization
ISR	Integrated SONET router
LACP	Link Aggregation Control Protocol
LACPDU	Link Aggregation Control Protocol data unit
LAN	local area network
LANE	LAN Emulation
LAPB	Link Access Procedure, Balanced
LCP	Link Control Protocol
LDA	Local Director Acceleration
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
LOU	logical operation units
LTL	Local Target Logic
MAC	Media Access Control
MD5	message digest 5
MDIX	media-dependent interface crossover
MDS	multicast distributed switching
MDSS	Multicast Distributed Shortcut Switching
MDT	multicast distribution tree
MFD	multicast fast drop
MFIB	multicast forwarding information base
mGRE	multipoint generic routing encapsulation
MIB	Management Information Base
MII	media-independent interface
MLDv2	multicast listener discovery version 2
MLS	Multilayer Switching
MLSE	maintenance loop signaling entity
MLSM	multilayer switching for multicast

**Table A-1** List of Acronyms (continued)

Acronym	Expansion
MN	mobile node
MOP	Maintenance Operation Protocol
MOTD	message-of-the-day
MPLS	Multiprotocol Label Switching
MQC	modular QoS CLI
mrinfo	multicast router information
MRM	multicast routing monitor
mroute	multicast route
mrouter	multicast router
MSDP	Multicast Source Discovery Protocol
MSM	Multilayer Switch Module
MSS	maximum segment size
MST	Multiple Spanning Tree (802.1s)
MSTCI	MST configuration identifier
MTU	maximum transmission unit
MVAP	multiple VLAN access port
NAM	Network Analysis Module
NAT	network address translation
NBMA	nonbroadcast multiaccess
NBP	Name Binding Protocol
NCIA	Native Client Interface Architecture
NDE	NetFlow Data Export
NDR	no drop rate
NET	network entity title
NetBIOS	Network Basic Input/Output System
NFFC	NetFlow Feature Card
NHRP	Next Hop Resolution Protocol
NMP	Network Management Processor
NSAP	network service access point
NSF	non-stop forwarding
NTP	Network Time Protocol
NVGEN	nonvolatile generation
NVRAM	nonvolatile RAM
OAL	optimized ACL logging
OAM	Operation, Administration, and Maintenance
ODM	order dependent merge

**Table A-1** *List of Acronyms (continued)*

<b>Acronym</b>	<b>Expansion</b>
OIF	Outgoing interface of a multicast {*,G} or {source, group} flow
OSI	Open System Interconnection
OSPF	open shortest path first
PAE	port access entity
PAgP	Port Aggregation Protocol
PBD	packet buffer daughterboard
P bits	prioritization bits
PBR	policy-based routing
PC	Personal Computer (formerly PCMCIA)
PCM	pulse code modulation
PCR	peak cell rate
PDP	policy decision point
PDU	protocol data unit
PE	provider edge
PEP	policy enforcement point
PE router	provider edge router
PFC	Policy Feature Card
PGM	Pragmatic General Multicast
PHY	physical sublayer
PIB	policy information base
PIR	peak information rate
PIM	protocol independent multicast
PIM-SM	Protocol Independent Multicast sparse mode
PISA	Programmable Intelligent Services Accelerator
PoS	Packet over Sonet
PPP	Point-to-Point Protocol
ppsec	packets per second
PRID	Policy Rule Identifiers
psecure	port security
PVL	per VLAN learning
PVLANs	private VLANs
PVST+	Per-VLAN Spanning Tree+
QDM	QoS device manager
QM	QoS manager
QM-SP	SP QoS manager
QoS	quality of service

**Table A-1 List of Acronyms (continued)**

Acronym	Expansion
QinQ	IEEE 802.1Q in 802.1Q
RACL	router interface access control list
RADIUS	Remote Access Dial-In User Service
RAM	random-access memory
RCP	Remote Copy Protocol
RF	Redundancy Facility
RGMP	Router-Ports Group Management Protocol
RIB	routing information base
RIF	Routing Information Field
RM	routed MAC
RMON	remote network monitor
ROM	read-only memory
ROMMON	ROM monitor
RP	route processor or rendezvous point
RPC	remote procedure call
RPF	reverse path forwarding
RPR	Route Processor Redundancy
RSPAN	remote SPAN
RST	reset
RSTP	Rapid Spanning Tree Protocol
RSTP+	Rapid Spanning Tree Protocol plus
RSVP	ReSerVation Protocol
RTP	Real-Time Transport Protocol
SA	source active
SAID	Security Association Identifier
SAP	service access point
SCM	service connection manager
SCP	Switch-Module Configuration Protocol or Serial Control Protocol
SDLC	Synchronous Data Link Control
SFP	small form factor pluggable
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

**Table A-1 List of Acronyms (continued)**

<b>Acronym</b>	<b>Expansion</b>
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
SREC	S-Record format, Motorola defined format for ROM contents
SRR	shaped round robin
SSL	Secure Sockets Layer
SSM	Source Specific Multicast
SSO	Stateful Switch Over
SSTP	Cisco Shared Spanning Tree
STP	Spanning Tree Protocol
SVC	switched virtual circuit
SVI	switched virtual interface
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
TDR	Time Domain Reflectometry
TFTP	Trivial File Transfer Protocol
TIA	Telecommunications Industry Association
TopN	Utility that allows the user to analyze port traffic by reports
ToS	type of service
TLV	type-length-value
TTL	Time To Live
TVX	valid transmission
UDE	unidirectional Ethernet
UDL	unidirectional link
UDLD	UniDirectional Link Detection Protocol
UDLR	UniDirectional Link Routing
UDP	User Datagram Protocol
UNI	User-Network Interface
uRPF	unicast reverse path forwarding

**Table A-1** *List of Acronyms (continued)*

<b>Acronym</b>	<b>Expansion</b>
UTC	Coordinated Universal Time
VACL	VLAN access control list
VCC	virtual channel circuit
VCI	virtual circuit identifier
VCR	Virtual Configuration Register
VFI	virtual forwarding instance
VINES	Virtual Network System
VLAN	virtual LAN
VMPS	VLAN Membership Policy Server
VMR	value mask result
VPLS	Virtual Private LAN Service
VPN	virtual private network
VRF	VPN routing and forwarding
VTP	VLAN Trunking Protocol
VVID	voice VLAN ID
WAN	wide area network
WCCP	Web Cache Coprocessor Protocol
WFQ	weighted fair queueing
WLSM	Wireless LAN Services Module
WRED	weighted random early detection
WRR	weighted round-robin
XCM	external column memory
XNS	Xerox Network System



## Acknowledgments for Open-Source Software

---

The Cisco IOS software on the Catalyst 6500 series switches software pipe command uses Henry Spencer's regular expression library (regex).

Henry Spencer's regular expression library (regex). Copyright 1992, 1993, 1994, 1997 Henry Spencer. All rights reserved. This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from flaws in it.
2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation.
3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation.
4. This notice may not be removed or altered.

The Cisco IOS software on the Catalyst 6500 series switches software pipe command uses Softfloat.

Softfloat was written by John R. Hauser. This work was made possible in part by the International Computer Science Institute, located at Suite 600, 1947 Center Street, Berkeley, California 94704. Funding was partially provided by the National Science Foundation under grant MIP-9311980. The original version of this code was written as part of a project to build a fixed-point vector processor in collaboration with the University of California at Berkeley, overseen by Profs. Nelson Morgan and John Wawrzynek. More information is available through the Web page <http://www.cs.berkeley.edu/~jhauser/arithmetic/SoftFloat.html>.

THIS SOFTWARE IS DISTRIBUTED AS IS, FOR FREE. Although reasonable effort has been made to avoid it, THIS SOFTWARE MAY CONTAIN FAULTS THAT WILL AT TIMES RESULT IN INCORRECT BEHAVIOR. USE OF THIS SOFTWARE IS RESTRICTED TO PERSONS AND ORGANIZATIONS WHO CAN AND WILL TAKE FULL RESPONSIBILITY FOR ALL LOSSES, COSTS, OR OTHER PROBLEMS THEY INCUR DUE TO THE SOFTWARE, AND WHO FURTHERMORE EFFECTIVELY INDEMNIFY JOHN HAUSER AND THE INTERNATIONAL COMPUTER SCIENCE INSTITUTE (possibly via similar legal warning) AGAINST ALL LOSSES, COSTS, OR OTHER PROBLEMS INCURRED BY THEIR CUSTOMERS AND CLIENTS DUE TO THE SOFTWARE.

Derivative works of Softfloat are acceptable, even for commercial purposes, so long as (1) the source code for the derivative work includes prominent notice that the work is derivative, and (2) the source code includes prominent notice with these four paragraphs for those parts of this code that are retained.





---

## Symbols

- # character (privileged EXEC mode prompt) [1-6](#)
- \$ character [1-8, 1-10](#)
- \* (asterisk) [1-8](#)
- + (plus sign) [1-8](#)
- . (period) [1-8](#)
- ? command [1-2](#)
- ^ (caret) [1-8, 1-10](#)
- \_ (underscore) [1-8, 1-11](#)
- | (pipe or vertical bar)
  - specifying alternative patterns [1-10](#)

---

## Numerics

- 802.1Q
  - disabling
    - tunneling [2-333](#)
  - displaying
    - enabled ports [2-694](#)
    - tunneled protocols [2-875](#)
  - enabling
    - tunneling [2-333](#)
  - encapsulation
    - disabling [2-128](#)
    - enabling [2-128](#)
  - mapping ISL VLANs [2-1276](#)
  - setting
    - CoS value [2-335](#)
    - drop threshold globally [2-338](#)
    - drop threshold on an interface [2-336](#)
    - maximum processed protocol packets [2-339](#)
    - mode [2-1195](#)
    - port interface type [2-1195](#)
    - setting trunk encapsulation characteristics [2-1209](#)
    - specifying
      - EtherType values [2-1193](#)
- 802.1Q tagging
  - disabling on VLANs [2-1270](#)
  - displaying information [2-1101](#)
  - enabling on VLANs [2-1270](#)
- 802.1s
  - See MST
- 802.1w
  - See RSTP+
- 802.1X
  - allowing multiple hosts [2-118](#)
  - default settings [2-116](#)
  - disabling
    - globally [2-122](#)
    - periodic authentication of client [2-121](#)
  - disallowing multiple hosts [2-118](#)
  - displaying
    - information for all interfaces [2-695](#)
  - enabling
    - globally [2-122](#)
    - periodic authentication of client [2-121](#)
  - resetting to defaults [2-116](#)
  - setting
    - authentication timer [2-123](#)
    - port control values [2-119](#)
    - reauthentication count [2-117](#)
- 802.3ad
  - See LACP
- 802.3af
  - configuring administrative mode [2-604](#)

## A

## abbreviating commands

- context-sensitive help [1-1](#)

## access control lists

- See ACLs

## accessing

- DFC-equipped modules [2-632](#)
- module-specific CLI [2-650](#)

## access lists

- IPX, time ranges [2-1227](#)

## access maps

- applying [2-1272](#)
- specifying sequence [2-380](#)

## acknowledgments for open-source software

- regular expression library [B-1](#)
- Softfloat [B-1](#)

## ACL counters

- displaying for packetswitched in hardware [2-1081](#)

## ACLs

## clearing

- counters [2-65](#)

- clearing statistical information [2-40](#)

## defining

- time ranges [2-1227](#)

## enabling

- time-based ACLs [2-1227](#)

## merge

- displaying current method [2-733](#)

## port access map

- creating [2-595](#)
- deleting [2-595](#)

## removing

- time limitation [2-1227](#)

## selecting

- BDD-based merge method [2-393](#)
- ODM-based merge method [2-393](#)

## TCAM

- setting default action during update [2-395](#)

- acronyms, list of [A-1](#)

## Address Resolution Protocol

- See ARP

## adjacency

## displaying

- node information [2-902](#)
- table information [2-661](#)

## aggregate counts

- missed flows [2-988](#)

## aggregate policer

- clearing statistics and token counts in high-rate and low-rate policer buckets [2-76](#)

- defining [2-458](#)

## MLS QoS

- enabling [2-495](#)

- removing [2-458](#)

## aggregate policers

## removing

- from current class [2-587](#)

## specifying

- for current class [2-587](#)

## aggressive UDLD

- See UDLD, aggressive mode

## aging time

- MAC address table [2-364](#)

## ARP

- displaying table [2-664](#)

## ARP ACL

- adding clauses [2-5](#)

## defining

- access list [2-5](#)

- entering submode [2-5](#)

- removing from list [2-5](#)

## ASIC

## displaying

- type [2-665](#)
- version [2-665](#)

- assigning an interface to a channel group [2-22](#)

## ATA flash

- restrictions [2-1171, 2-1248](#)
- audience [xxv](#)
- authentication
  - setting username [2-1254](#)
- authentication proxy
  - watch list
    - adding IP address [2-181](#)
    - clearing entries [2-43](#)
    - configuring [2-181](#)
    - disabling [2-181](#)
    - displaying [2-782](#)
    - enabling [2-181](#)
    - setting maximum login attempts [2-179](#)
- authorization traps during unknown context error
  - disabling [2-1129](#)
  - enabling [2-1129](#)
- autonegotiation
  - setting delay timer [2-1219](#)

---

## B

- BDD
  - selecting ACL merge method [2-393](#)
- BGP
  - configuring maximum number of parallel routes [2-385](#)
  - enabling
    - deterministic processing time regular expression engine [2-11](#)
    - regular expression engine [2-11](#)
- Bidir
  - configuring
    - RP RPF scan interval [2-425](#)
  - displaying
    - cached rendezvous points [2-858](#)
    - DF interface information [2-848](#)
    - information [2-947](#)
    - IP multicast routing table information [2-834](#)
    - IP multicast table information [2-829, 2-834](#)
- bidirectional CDP

- configuring administrative mode [2-604](#)
- bidirectional PIM
  - See BIDIR
- binary decision diagrams
  - See BDD
- boot configuration file
  - returning to default location [2-13](#)
  - specifying device and filename [2-13](#)
- BOOT environment variable
  - displaying information [2-668](#)
  - specifying [2-15](#)
- bootflash
  - file system, displaying information [2-666](#)
- booting
  - from Flash [2-15](#)
- boot system command [2-15](#)
- Border Gateway Protocol
  - See BGP
- BPDU
  - conversion over protocol tunneling links [2-18](#)
- BPDU filtering
  - disabling
    - by default [2-1158](#)
    - on an interface [2-1132](#)
  - enabling
    - by default [2-1158](#)
    - on an interface [2-1132](#)
- BPDU guard
  - disabling
    - by default [2-1160](#)
    - on an interface [2-1134](#)
  - enabling
    - by default [2-1160](#)
    - on an interface [2-1134](#)
- bridged flows
  - disabling
    - globally for NDE [2-216](#)
    - inbound NDE [2-215](#)
  - enabling

- globally for NDE [2-216](#)
  - inbound NDE [2-215](#)
  - bridged traffic
    - microflow policing [2-460](#)
  - bridge protocol data unit
    - See BPDUs
  - byte count, displaying [2-750](#)
- 
- ## C
- cable diagnostics
    - TDR
      - clearing all interfaces [2-33](#)
      - clearing specific interface [2-33](#)
      - displaying test results [2-671](#)
      - running test [2-1225](#)
  - CAM table usage monitoring
    - disabling [2-371](#)
    - enabling [2-371](#)
  - CASA
    - configuring
      - function as a forwarding agent [2-183](#)
    - disabling
      - function as a forwarding agent [2-183](#)
  - CDP
    - displaying
      - neighbor information [2-675](#)
  - CEF
    - clearing
      - IP per-prefix accounting statistics [2-67](#)
      - IPv6 per-prefix accounting statistics [2-68](#)
    - consistency checker parameters
      - disabling [2-185](#)
      - enabling [2-185](#)
    - consistency checker types
      - disabling [2-185](#)
      - enabling [2-185](#)
    - disabling
      - MLS per-prefix accounting [2-410](#)
      - rate-limiting [2-413](#)
      - tunnel fragmentation [2-402](#)
    - displaying
      - IPv4 unicast address [2-914, 2-929](#)
      - maximum route system configuration [2-930](#)
      - next-hop information [2-798](#)
      - VLAN configuration information [2-798](#)
      - VLAN interface status [2-798](#)
    - enabling
      - missing prefix detection [2-185](#)
      - MLS per-prefix accounting [2-410](#)
      - rate-limiting [2-413](#)
      - tunnel fragmentation [2-402](#)
    - epoch
      - beginning new epoch [2-44](#)
      - displaying information [2-793](#)
      - incrementing [2-44](#)
    - inconsistencies
      - clearing [2-46](#)
      - displaying [2-795](#)
    - selecting
      - load-balancing algorithm [2-184](#)
    - setting
      - checker type [2-185](#)
      - elapsed time [2-185](#)
      - load balancing [2-411](#)
      - period between scans [2-185](#)
      - rate-limiting [2-413](#)
      - route limiting per protocol [2-400](#)
    - specifying
      - maximum number of prefixes to check per scan [2-185](#)
      - passive scan check [2-185](#)
  - changing to untrusted port state [2-484, 2-503](#)
  - chassis
    - displaying
      - chassis MAC address ranges [2-673](#)
      - current and peak traffic meter readings [2-673](#)
      - model type [2-740](#)
      - percentage of backplane utilization [2-673](#)

- product number [2-740](#)
  - serial number [2-740](#)
  - switching clock failure recovery mode [2-673](#)
- chassis serial number, displaying [2-738](#)
- checksum
  - computing
    - MD5 signature [2-1255](#)
  - verifying
    - compressed image [2-138](#)
    - Flash memory file [2-1255](#)
- CIR
  - setting rate [2-458](#)
- circular cache-header buffer, displaying contents [2-827](#)
- Cisco Appliance Services Architecture
  - See [CASA](#)
- Cisco Express Forwarding
  - See [CEF](#)
- Cisco IOS VLAN subinterface
  - displaying information [2-1110](#)
- class (policy-map) command [2-30](#)
- class map
  - configuring
    - match criteria on IP packets [2-382](#)
    - match criteria on IPv6 packets [2-382](#)
    - match criteria per protocol [2-382](#)
  - displaying information [2-679](#)
- MLS QoS
  - enabling [2-497](#)
- removing
  - match criteria per protocol [2-382](#)
- class maps
  - configuration mode
    - accessing [2-26](#)
- class policies
  - configuring [2-30](#)
  - default class, configuring [2-30](#), [2-593](#)
- clearing a Gigabit Ethernet interface [2-38](#)
- CLI
  - accessing
    - module-specific CLI [2-632](#)
    - remote login [2-632](#)
  - string search
    - alternation [1-10](#)
    - anchoring [1-10](#)
    - expressions [1-7](#)
    - filtering [1-7](#)
    - multiple-character patterns [1-9](#)
    - multipliers [1-9](#)
    - parentheses for recall [1-11](#)
    - searching outputs [1-7](#)
    - single-character patterns [1-8](#)
    - using [1-7](#)
  - client ID [2-1048](#)
- CNS
  - Cisco Networking Services
    - See [online diagnostics](#)
- command-line interface
  - See [CLI](#)
- command modes
  - accessing [1-5](#)
  - exiting [1-5](#)
  - understanding [1-5](#)
- commands
  - executing multiple interfaces simultaneously [2-162](#)
  - mode types [1-5](#)
- committed information rate
  - See [CIR](#)
- compression mode
  - turning off [2-439](#)
  - turning on [2-439](#)
- configuration
  - entering line configuration collection mode [2-346](#)
  - specifying terminal line [2-346](#)
- configuration, saving [1-11](#)
- connection attempted by a failed server
  - changing to defaults [2-636](#)
  - defining elapsed times [2-636](#)
- consistency checker

- configuring [2-428](#)
  - disabling [2-428](#)
  - displaying
    - information [2-944](#)
  - enabling [2-428](#)
  - Content Switching Module
    - See CSM
  - control plane policing
    - See CoPP
  - cooling
    - displaying information [2-702](#)
  - CoPP
    - attaching
      - policy map to control plane [2-648](#)
    - configuring
      - traffic policing [2-590](#)
    - displaying
      - policy-map class information [2-1038](#)
    - entering configuration mode [2-92](#)
    - removing
      - service policy from control plane [2-648](#)
  - copying files [2-94](#)
    - enabling automatic checksum verification [2-138](#)
    - validating image [2-138](#)
  - copy inner to out .1pbits
    - configuring [2-468](#)
    - deleting an entry [2-468](#)
  - CoS
    - inner CoS to outer CoS translation
      - displaying configuration information [2-975](#)
      - displaying runtime version information [2-975](#)
      - mapping [2-468](#)
  - CoS mutation maps
    - attaching to interface [2-463](#)
    - removing from interface [2-463](#)
  - CoS to CoS
    - attaching
      - CoS mutation map to interface [2-463](#)
    - removing
      - CoS mutation map from interface [2-463](#)
  - CoS to CoS mapping
    - configuring [2-468](#)
  - CoS value
    - defining default value [2-462](#)
  - CoS values
    - mapping to strict-priority queue [2-606](#)
    - returning to default mappings [2-606](#)
  - counters
    - clearing hardware interface counters [2-35](#)
    - clearing interface counters [2-35](#)
    - clearing NetFlow counters [2-37](#)
    - displaying
      - interface counter information [2-680](#)
  - CPU time
    - guaranteeing processing time [2-645](#)
  - CSM
    - shutting down [2-153](#)
  - custom EtherTypes
    - specifying EtherType values [2-1193](#)
- 
- D
- DAI
    - adding
      - clauses to ARP ACL [2-5](#)
    - applying ARP ACL to VLAN [2-167](#)
    - clearing
      - log buffer status [2-41](#)
      - statistics [2-42](#)
    - configuring
      - IP ARP log buffer [2-171](#)
    - defining
      - ARP ACL [2-5](#)
    - disabling
      - globally [2-176](#)
      - IP ARP inspection checks [2-174](#)
    - displaying
      - log buffer status [2-780](#)

- status for VLANs [2-777](#)
- DoS protection [2-169](#)
- enabling
  - globally [2-176](#)
  - IP ARP inspection checks [2-174](#)
- entering ARP ACL submode [2-5](#)
- removing
  - ARP ACL [2-5](#)
- setting
  - per-port configurable trust state [2-173](#)
- dead process statistics, displaying [2-894](#)
- debounce timer
  - configuring [2-348](#)
  - disabling [2-348](#)
  - displaying debounce timer configuration [2-753](#)
  - enabling [2-348](#)
- default form of a command, using [1-7](#)
- delimiter
  - configuring for MLS QoS [2-499](#)
- denial of service
  - See DoS
- designated forwarder
  - See DF
- destination address
  - MLS QoS
    - setting statistics data export destination address [2-500](#)
- deterministic processing time regular expression engine
  - disabling [2-11](#)
  - enabling [2-11](#)
- DF
  - displaying interface information [2-848](#)
- DFC
  - remote login
    - remote login command [2-632](#)
- DHCP
  - clearing
    - snooping binding entries [2-47](#)
    - snooping database entries [2-47](#)
    - snooping statistical entries [2-47](#)
  - disabling
    - all interfaces as trusted sources [2-187](#)
    - interface as a trusted source [2-188](#)
  - displaying
    - configured trusted interfaces [2-799](#)
  - enabling
    - all interfaces as trusted sources [2-187](#)
    - interface as a trusted source [2-188](#)
  - snooping binding
    - clearing table entries [2-47](#)
  - snooping database
    - clearing table entries [2-47](#)
  - snooping statistical
    - clearing table entries [2-47](#)
  - specifying
    - connected routes [2-189](#)
- DHCP bindings
  - configuring bindings [2-191](#)
- DHCP snooping
  - configuring
    - abort timeout interval [2-193](#)
    - database [2-193](#)
    - number of DHCP messages received [2-197](#)
    - write-delay time [2-193](#)
  - disabling
    - global [2-190](#)
    - MAC address comparison [2-199](#)
    - on a group of VLANs [2-200](#)
    - on a VLAN [2-200](#)
    - tunnel interface [2-198](#)
  - displaying
    - binding table entries [2-802](#)
    - configuration information [2-800](#)
    - DHCP database status [2-805](#)
    - statistical information [2-800](#)
  - enabling
    - global [2-190](#)
    - MAC address comparison [2-199](#)
    - on a group of VLANs [2-200](#)

- on a VLAN [2-200](#)
  - tunnel interface [2-198](#)
- enabling option 82 [2-195](#)
- establishing binding configuration [2-191](#)
- specifying
  - URL for storing entries [2-193](#)
- digital optical monitoring
  - See DOM
- directed broadcasts
  - disabling [2-418](#)
  - displaying information [2-902](#)
  - enabling [2-418](#)
- directories
  - creating [2-392](#)
  - setting the default [2-20](#)
- disabling DNS lookups [2-240](#)
- Distributed Forwarding Card
  - See DFC
- documentation
  - conventions [xxvi](#)
  - organization [xxv](#)
- DOM
  - disabling
    - transceiver traps [2-1124](#)
  - displaying
    - transceivers operational information [2-768](#)
    - transceivers threshold violations [2-768](#)
  - enabling
    - transceiver traps [2-1124](#)
- DoS
  - configuring
    - traffic policing [2-590](#)
- CoPP
  - attaching policy map to control plane [2-648](#)
  - displaying policy-map class information [2-1038](#)
  - entering configuration mode [2-92](#)
  - removing service policy from control plane [2-648](#)
- disabling
  - rate limiting [2-413](#)
- enabling
  - rate limiting [2-413](#)
- entering
  - CoPP configuration mode [2-92](#)
- setting
  - rate limits [2-413](#)
- DoS protection
  - ARP broadcast [2-487](#)
- configuring
  - IPv4 multicast rate limiters [2-511](#)
  - IPv6 multicast rate limiters [2-513](#)
- configuring DAI [2-169](#)
- disabling
  - IPv4 multicast rate limiters [2-511](#)
  - IPv6 multicast rate limiters [2-513](#)
- displaying information [2-982](#)
- rate limiters
  - configuring CEF rate limiters [2-518](#)
  - configuring for ACL-bridged rate limiters [2-516](#)
  - configuring for Layer 3 security rate limiters [2-523](#)
  - configuring for unicast packets [2-520](#)
  - configuring for VACL-log cases [2-524](#)
  - disabling [2-508](#)
  - disabling CEF rate limiters [2-518](#)
  - disabling for ACL-bridged rate limiters [2-516](#)
  - disabling for Layer 3 security rate limiters [2-523](#)
  - disabling for unicast packets [2-520](#)
  - displaying information [2-982](#)
  - enabling [2-508](#)
  - enabling CEF rate limiters [2-518](#)
  - enabling for ACL-bridged rate limiters [2-516](#)
  - enabling for Layer 3 security rate limiters [2-523](#)
  - enabling for unicast packets [2-520](#)
  - enabling for VACL-log cases [2-524](#)
  - rate limiters for VACL-log cases
    - disabling for VACL-log cases [2-524](#)
- dot1q
  - See also 802.1Q
- dot1x

- See 802.1x
  - double-tagged Q-in-Q
    - See QinQ
  - DSCP
    - attaching
      - DSCP mutation map to interface [2-464](#)
    - defining
      - mutation mapping [2-473](#)
    - displaying
      - mutation mapping [2-970](#)
    - removing
      - DSCP mutation map from interface [2-464](#)
  - DSCP mutation maps
    - attaching to interface [2-464](#)
    - removing from interface [2-464](#)
  - DSS
    - displaying range invalidation profile [2-698](#)
  - dualmode uplink
    - selecting connector type [2-391](#)
  - duplex mode
    - configuring [2-125](#)
  - DWRR queues
    - configuring
      - bandwidth [2-1281](#)
  - dynamic ARP inspection
    - See DAI
  - Dynamic Host Configuration Protocol
    - See DHCP snooping
  - dynamic MAC address entries
    - clearing [2-63](#)
  - dynamic SVI
    - accessing [2-164](#)
    - creating [2-164](#)
    - deleting [2-164](#)
- 
- E
- egress
    - attaching
      - DSCP mutation map to interface [2-464](#)
    - defining
      - DSCP mutation mapping [2-473](#)
      - DSCP-to-CoS mapping [2-470](#)
      - DSCP-to-DSCP mapping [2-473](#)
      - DSCP-to-EXP mapping [2-472](#)
      - EXP mutation mapping [2-476](#)
      - EXP-to-EXP mapping [2-476](#)
      - ingress-EXP-to-DSCP mapping [2-475](#)
    - deleting
      - DSCP-to-CoS mapping [2-470](#)
      - DSCP-to-DSCP mapping [2-473](#)
      - DSCP-to-EXP mapping [2-472](#)
      - EXP-to-EXP mapping [2-476](#)
      - ingress-EXP-to-DSCP mapping [2-475](#)
    - displaying
      - DSCP mutation mapping [2-970](#)
      - mode information [2-944](#)
      - queueing information [2-1051](#)
    - removing
      - DSCP mutation map from interface [2-464](#)
  - egress replication capability [2-422](#)
  - EIGRP
    - setting
      - event log size [2-127](#)
  - enabling
    - routing [2-277](#)
  - encapsulation
    - 802.1Q
      - disabling [2-128](#)
      - enabling [2-128](#)
    - ISL
      - disabling [2-129](#)
      - enabling [2-129](#)
  - Enhanced Address Recognition Logic
    - See EARL
  - enhanced password security
    - establishing [2-1254](#)
  - entering VLAN-configuration submode [2-1268](#)

- environmental alarms
  - displaying information [2-699](#)
- environment variables
  - BOOT, specifying [2-15](#)
- EoBC interface
  - displaying information [2-708](#)
- EoMPLS
  - disabling
    - routing [2-565](#)
    - VLAN based forwarding [2-565](#)
  - enabling
    - routing [2-565](#)
    - VLAN based forwarding [2-565](#)
- epoch
  - displaying information [2-793](#)
  - incrementing [2-44](#)
  - rebuilding CEF table [2-44](#)
- error counters
  - displaying summary [2-1084](#)
- error detection
  - setting
    - module action during packet buffer memory failures [2-136](#)
- error disable
  - detection
    - configuring timer [2-132](#)
    - packet buffer errors [2-132](#)
    - specifying recovery cause [2-132](#)
  - recovery
    - configuring timer [2-134](#)
    - displaying information [2-714](#)
    - specifying recovery cause [2-134](#)
  - state
    - displaying information [2-760](#)
- error disable detection
  - displaying information [2-712, 2-713](#)
- ERSPAN
  - adding interfaces or VLANs [2-560](#)
  - deleting interfaces or VLANs [2-560](#)
- deleting session [2-560](#)
- displaying
  - session information [2-1002](#)
- ending session [2-555](#)
- entering destination-session configuration mode [2-555](#)
- entering source-session configuration mode [2-555](#)
- starting new session [2-560](#)
- starting session [2-555](#)
- tables
  - destination session configuration mode syntaxes [2-561](#)
  - source session configuration mode syntaxes [2-562](#)
- EtherChannel
  - assigning interface to an EtherChannel group [2-22](#)
  - displaying
    - information [2-715](#)
  - guard misconfiguration detection
    - detecting [2-1136](#)
    - disabling [2-1136](#)
    - enabling [2-1136](#)
    - error message [2-1136](#)
  - minimum links
    - setting [2-601](#)
  - removing interface from an EtherChannel group [2-22](#)
- Ethernet over Multiprotocol Label Switching
  - See EoMPLS
- EtherTypes
  - specifying values [2-1193](#)
- event tracing
  - configuring
    - global configuration mode [2-550](#)
    - privileged EXEC mode [2-547](#)
- Exception Recovery Manager
  - See ERM
- EXEC-level commands
  - issuing in other modes [2-115](#)
- executing remote switch command [2-631](#)
- explicit host tracking
  - disabling [2-224](#)

- enabling [2-224](#)
  - explicit tracking
    - disabling for MLDv2 snooping [2-314](#)
    - displaying
      - database [2-873](#)
    - displaying information [2-990](#)
    - enabling for MLDv2 snooping [2-314](#)
    - IGMP snooping
      - limiting size of database [2-232](#)
    - MLDv2 snooping
      - limiting size of database [2-318](#)
  - EXP MAP
    - attaching
      - EXP mutation map to interface [2-465](#)
    - removing
      - EXP mutation map from interface [2-465](#)
  - EXP mutation maps
    - attaching to interface [2-465](#)
    - removing from interface [2-465](#)
  - export interval
    - MLS QoS
      - setting [2-502](#)
  - expressions
    - matching multiple expression occurrences [1-9](#)
    - multiple-character patterns [1-9](#)
    - multiplying pattern occurrence [1-11](#)
    - single-character patterns [1-8](#)
    - specifying alternative patterns [1-10](#)
  - extended MAC access list
    - defining [2-361](#)
  - extended-range VLANs
    - configuring
      - characteristics in capture mode [2-1191](#)
      - STP [2-1166](#)
    - creating dynamic SVI [2-164](#)
    - defining
      - PVLAN association [2-1206](#)
    - deleting
      - dynamic SVI [2-164](#)
  - ERSPAN session [2-560](#)
  - PVLAN association [2-1206](#)
  - RSPAN session [2-555](#)
  - SPAN session [2-555](#)
  - disabling capture mode [2-1189](#)
  - displaying
    - current operating information [2-1059](#)
    - filter information [2-1102](#)
  - enabling capture mode [2-1189](#)
  - entering config-VLAN mode [2-1262](#)
  - executing a command on multiple interfaces [2-162](#)
  - setting
    - when in access mode [2-1182](#)
  - starting
    - new ERSPAN session [2-560](#)
    - new RSPAN session [2-555](#)
    - new SPAN session [2-555](#)
  - extended system ID display
    - disabling [2-1138](#)
    - enabling [2-1138](#)
  - external column memory
    - See XCM
- 
- ## F
- fan trays
    - displaying part number [2-703](#)
  - fan-trays
    - setting version [2-150](#)
  - fast software upgrade
    - See FSU
  - feature interaction engine
    - See FIE
  - feature manager
    - displaying
      - CBAC-configured ACL lists and ports [2-723](#), [2-731](#)
      - dynamic reflexive entries [2-732](#)
      - general information [2-720](#)
      - inband packet count [2-722](#)

- per-interface information [2-724, 2-727](#)
    - per-VLAN information [2-734](#)
    - summaries [2-733](#)
  - FIB TCAM exception
    - displaying status for IPv4, IPv6, and MPLS protocols [2-711](#)
  - FIB usage
    - displaying [2-935](#)
  - field [A-4](#)
  - field programmable devices
    - See FPD
  - field-replaceable unit
    - See FRU
  - field upgradeable ROMMON
    - upgrading
      - route processor [2-1252](#)
      - switch processor [2-1252](#)
  - files
    - copying [2-94](#)
    - disabling automatic image verification [2-94](#)
    - enabling automatic checksum verification [2-138](#)
    - validating image [2-138](#)
  - file system
    - erase [2-130](#)
  - file system consistency check
    - See fsck utility
  - Firewall Services Module
    - See FWSM
  - Flash file system
    - check and repair [2-144](#)
    - checking for damage [2-144](#)
    - creating new directory [2-392](#)
    - directory recovery [2-1248](#)
    - enabling fsck utility [2-144](#)
    - file recovering [2-1248](#)
    - format [2-141](#)
    - permanently deleting files [2-1171](#)
    - setting the default [2-20](#)
    - verify checksum [2-1255](#)
  - Flash memory
    - booting automatically [2-15](#)
    - formatting [2-141](#)
  - Flexlink
    - disabling [2-1186](#)
    - displaying
      - Flexlink pairs [2-766](#)
    - enabling [2-1186](#)
  - flow control
    - configuring receive mode [2-139](#)
    - configuring send mode [2-139](#)
    - displaying configuration information [2-756](#)
    - port guidelines [2-140](#)
  - flow fragments
    - permit configuration [2-166](#)
  - flow mask
    - restoring [2-407](#)
    - specifying [2-407](#)
  - fm
    - See feature manager
  - Frame Relay
    - displaying traffic [2-742](#)
    - specifying
      - interval to calculate average load [2-350](#)
  - Frame Relay MIB enhancement
    - specifying
      - interval to calculate average load [2-350](#)
  - FRU
    - displaying IDPROM information [2-738](#)
    - displaying status information [2-703](#)
  - fsck utility
    - enabling [2-144](#)
    - setting automatic mode [2-144](#)
  - FSU
    - redundancy force-switchover command [2-628](#)
- 
- G
- GBIC

- displaying type [2-747](#)
  - GBTE
    - displaying tunnel information [2-1010](#)
  - Gigabit Ethernet interface
    - clearing hardware logic [2-38](#)
  - Gigabit Ethernet WAN
    - See GE-WAN
  - global configuration mode, summary [1-6](#)
  - group cache entries
    - clearing [2-49](#)
  - Guaranteed Bandwidth TE
    - See GBTE
- 
- ## H
- half-duplex mode
    - configuring [2-125](#)
  - hardware
    - displaying
      - FIB TCAM exception status [2-711](#)
      - verifying programmed values [2-1049](#)
  - hardware ACL counters
    - displaying information for packets switched in hardware [2-1081](#)
  - hardware interface counters
    - clearing [2-35](#)
  - hardware Layer 3 switching
    - disabling
      - tunnel fragmentation [2-402](#)
    - displaying
      - adjacency node information [2-902](#)
      - adjacency table information [2-661](#)
      - entry information [2-897](#)
      - exception status [2-908](#)
      - hardware load-sharing information [2-907](#)
      - hardware table entry information [2-910](#)
      - IP entry information [2-914](#)
      - maximum route system configuration [2-930](#)
      - number of prefixes in hardware Layer 3 switching table [2-935](#)
      - packet information [2-935](#)
      - priority information [2-908](#)
      - RPF information [2-933](#)
      - statistical information [2-934](#)
      - TCAM entry index information [2-914, 2-929](#)
  - enabling
    - tunnel fragmentation [2-402](#)
  - HSRP [2-1177](#)
  - setting
    - route limiting per protocol [2-400](#)
  - hardware logic
    - clearing on VLANs [2-39](#)
  - hardware resources
    - displaying information [2-1020](#)
  - hardware switching
    - configuring
      - consistency checker [2-428](#)
      - flow statistics message from SP to RP [2-430](#)
    - disabling
      - checksum error checking [2-538](#)
      - consistency checker [2-428](#)
      - globally [2-536](#)
      - ingress replication mode [2-431](#)
      - Layer 3 error checking [2-538](#)
      - length consistency check [2-538](#)
      - unicast traffic [2-537](#)
    - displaying
      - (\* ,G) shortcuts [2-918](#)
      - Bidir information [2-918](#)
      - CEF table information [2-797](#)
      - CEF table information in compact format [2-918](#)
      - consistency checker information [2-944](#)
      - information based on (\* ,G/m) entries [2-918](#)
      - information based on (S,G) shortcuts [2-918](#)
      - information based on Bidir (\* ,G/m) shortcuts [2-918](#)
      - information based on group address [2-918](#)
      - information based on IP subnet prefix [2-918](#)

- information based on RPF VLAN ID [2-918](#)
  - information based on source IP [2-918](#)
  - multicast replication capabilities [2-944](#)
  - VRF CEF table information [2-937](#)
  - enabling
    - checksum error checking [2-538](#)
    - consistency checker [2-428](#)
    - globally [2-536](#)
    - ingress replication mode [2-431](#)
    - Layer 3 error checking [2-538](#)
    - unicast traffic [2-537](#)
  - health monitoring diagnostic tests
    - configuring [2-104](#)
  - helper addresses, IP [2-822](#)
  - host connection
    - optimizing port configuration [2-1180](#)
  - Hot Standby Router Protocol
    - See HSRP
  - HSRP
    - configuring
      - hardware Layer 3 switching [2-1177](#)
      - initialization delay [2-1173](#)
      - tracking [2-1175](#)
    - disabling
      - delay period [2-1173](#)
    - displaying
      - delay period information [2-1074](#)
  - ifIndex persistence
    - clearing previously interface configuration mode SNMP ifIndex commands [2-1118](#)
    - disabling globally [2-1125](#)
    - disabling on an interface [2-1120](#)
    - enabling globally [2-1125](#)
    - enabling on an interface [2-1120](#)
  - IGMP
    - clearing IGMP group cache entries [2-49](#)
    - configuring
      - last member query interval [2-220](#)
    - disabling
      - proxy reporting [2-224](#)
    - displaying
      - explicit tracking information [2-990](#)
      - explicit-tracking status [2-812](#)
      - interface configuration information [2-812](#)
      - interface status information [2-812](#)
      - multicast groups [2-809](#)
      - snooping information for VLAN interface [2-812](#)
      - status and configuration information [2-812](#)
      - status and configuration information for VLAN [2-812](#)
    - explicit host tracking
      - disabling [2-224](#)
      - enabling [2-224](#)
    - rate limit
      - setting [2-237, 2-318](#)
    - snooping
      - clearing statistical information [2-51](#)
      - configuring a Layer 2 port as a multicast router port [2-233](#)
      - configuring fast leave [2-226](#)
      - configuring last member query interval [2-230](#)
      - disabling [2-222](#)
      - displaying information [2-815](#)
      - displaying rate limit information [2-816](#)
      - displaying statistical information [2-817](#)
      - enabling [2-222](#)
      - enabling multicast support within a subnet [2-235](#)
- 
- ICC
    - displaying counter and status information [2-736](#)
  - ICMPv6 neighbor-discovery ACLs
    - disabling
      - TCAM support optimization [2-583](#)
    - enabling
      - TCAM support optimization [2-583](#)
  - IDPROM
    - displaying information [2-738](#)

- enabling querier function [2-235](#)
- limiting size of explicit tracking database [2-232](#)
- maximum number of Layer 2 entries [2-229](#)
- periodic flooding of multicast packets [2-239](#)
- setting incoming message rate limit [2-237, 2-318](#)
- IGMP snooping
  - configuring
    - last member query interval [2-230](#)
    - maximum number of Layer 2 entries [2-229](#)
  - disabling [2-222](#)
    - explicit host tracking [2-224](#)
    - fast leave processing [2-226](#)
    - multicast support within a subnet [2-235](#)
  - enabling [2-222](#)
    - explicit host tracking [2-224](#)
    - fast leave processing [2-226](#)
    - multicast support within a subnet [2-235](#)
  - multicast router
    - learning method, configuring [2-233](#)
    - next-hop interface, specifying [2-233](#)
- images
  - disabling verification for current operation [2-94](#)
  - enabling automatic checksum verification [2-138](#)
  - validating image [2-138](#)
- inactive state
  - displaying reason for the inactive state [2-760](#)
- informs, enabling [2-1122](#)
- ingress
  - attaching
    - CoS mutation map to interface [2-463](#)
    - EXP mutation map to interface [2-465](#)
  - defining
    - CoS-to-DSCP mapping [2-467](#)
  - defining IP precedence-to-DSCP mapping [2-478](#)
  - deleting
    - CoS-to-DSCP mapping [2-467](#)
  - deleting IP precedence-to-DSCP mapping [2-478](#)
  - displaying
    - queueing information [2-1051](#)
  - removing
    - CoS mutation map from interface [2-463](#)
    - EXP mutation map from interface [2-465](#)
- inline power
  - configuring administrative mode [2-604](#)
  - displaying
    - power consumed by module [2-1044](#)
    - status information [2-1044](#)
- inner CoS to outer CoS translation
  - defining [2-468](#)
  - displaying [2-975](#)
    - mapping [2-975](#)
- instance numbering
  - mapping [2-155](#)
  - returning to default [2-155](#)
- inter-card communication
  - See ICC
- interface accounting information, displaying [2-745](#)
- interface configuration mode
  - entering [2-157](#)
  - summary [1-6](#)
  - table defining modes [1-6](#)
- interface counters
  - displaying information [2-680](#)
- interface-range macro
  - creating [2-97](#)
- interfaces
  - configuring
    - duplex mode [2-125](#)
    - half-duplex mode [2-125](#)
    - interface speeds [2-1168](#)
  - displaying
    - accounting information [2-745](#)
    - administrative status [2-764, 2-766](#)
    - description [2-755](#)
    - error counters [2-750](#)
    - error-disabled state [2-760](#)
    - flow control information [2-756](#)
    - interface capabilities [2-747](#)

- operation status [2-764, 2-766](#)
- PVLAN mapping [2-759](#)
- status [2-755](#)
- status summary [2-762](#)
- total number of interface VLANs [2-762](#)
- total suppression discard counts [2-750](#)
- traffic [2-742](#)
- trunk counters [2-750](#)
- trunk information [2-771](#)
- entering interface configuration mode [2-157](#)
- switching ports
  - displaying administrative and operational status [2-764](#)
  - displaying Flexlink pairs [2-766](#)
  - displaying status [2-764, 2-766](#)
- intermediate system-to-intermediate system
  - See IS-IS
- internal VLAN allocation
  - configuring [2-1274](#)
  - default setting [2-1274](#)
  - displaying
    - allocation information [2-1104](#)
- internal VLANs
  - displaying status [2-1093](#)
- Internet Group Management Protocol
  - See IGMP
- Internetwork Packet Exchange
  - See IPX
- inter packet gap
  - See IPG
- interprocessor communication
  - See IPC
- interrupt throttling
  - clearing
    - counters [2-81](#)
  - displaying
    - information [2-1016](#)
- Inter-Switch Link VLANs
  - See ISL VLANs
- IP
  - clearing
    - access list statistical information [2-40](#)
  - displaying interface usability status [2-821](#)
  - displaying IPv4 unicast address [2-914, 2-929](#)
  - NetFlow
    - enabling switching [2-304](#)
- IP ARP
  - applying ARP ACL to VLAN [2-167](#)
  - clearing
    - DAI statistics [2-42](#)
    - log buffer status [2-41](#)
  - configuring
    - log buffer [2-171](#)
  - controlling packet logging [2-177](#)
  - disabling
    - DAI [2-176](#)
    - inspection check [2-174](#)
  - displaying
    - DAI status [2-777](#)
    - log buffer status [2-780](#)
  - enabling
    - dynamic inspection [2-176](#)
    - inspection check [2-174](#)
  - limiting rate of incoming requests [2-169](#)
  - log buffer
    - clearing status [2-41](#)
    - displaying status [2-780](#)
  - setting
    - per-port configurable trust state [2-173](#)
  - trust state
    - setting [2-173](#)
- IPC
  - displaying cache flow entries [2-785](#)
- IP fast-switching cache, displaying contents [2-824](#)
- IPG
  - returning to default mode [2-165](#)
  - setting mode [2-165](#)
- IP IGMP

- See IGMP
- IP multicast [2-277](#)
  - allocating circular buffer storage [2-269](#)
  - allowing
    - routing between broadcast-only internetworks [2-271](#)
  - Bidir
    - clearing entries [2-69](#)
  - configuring
    - administratively scoped boundary [2-267](#)
  - deleting
    - group [2-70](#)
  - disabling
    - load splitting across multiple paths [2-274](#)
    - routing [2-277](#)
  - enabling
    - load splitting across multiple paths [2-274](#)
  - filtering
    - multicast router information request packets [2-273](#)
  - filtering auto RP messages [2-267](#)
  - limiting number of routes added to table [2-276](#)
  - removing
    - administratively scoped boundary [2-267](#)
    - circular buffer [2-269](#)
  - routing
    - displaying routing table [2-829, 2-834](#)
    - displaying snooping information [2-815](#)
  - statistic counters
    - resetting [2-71](#)
- IP multicast routing
  - MRM
    - UDP port numbers [2-1247](#)
  - mroute, configuring [2-243](#)
  - packet headers, storing [2-269, 2-828](#)
  - PIM
    - neighbors, displaying [2-854](#)
    - shortest path tree, delaying use [2-299](#)
  - RP
    - address, configuring [2-282](#)
    - Auto-RP, groups covered [2-292, 2-293](#)
    - Auto-RP, mapping agent [2-295](#)
    - filter RP announcements [2-290](#)
    - PIM Version 2 candidate, advertising [2-291](#)
  - See also mroute
- IP output queue
  - limiting size [2-147](#)
  - restoring default size [2-147](#)
- IP processing
  - disabling [2-309](#)
  - enabling [2-309](#)
- IP-routing protocols
  - configuring maximum number of parallel routes [2-385](#)
- IP shortcuts to MSFC
  - disabling [2-526](#)
  - enabling [2-526](#)
- IPv4
  - clearing
    - software-installed entries [2-73](#)
  - configuring
    - multicast rate limiters [2-511](#)
  - disabling
    - multicast rate limiters [2-511](#)
  - displaying
    - FIB TCAM exceptions [2-711](#)
    - information [2-940](#)
- IPv6
  - ACLs
    - displaying hardware NetFlow IPv6 configuration [2-967](#)
    - displaying NetFlow entries for reflexive ACLs [2-957](#)
    - enabling compression mode [2-439](#)
  - clearing
    - per-prefix accounting statistics [2-68](#)
    - software-installed entries [2-73](#)
  - configuring
    - multicast rate limiters [2-513](#)
    - NDE flow mask [2-407](#)
  - disabling
    - CEF-based multicast forwarding [2-311](#)

- compression mode [2-439](#)
  - denial of packets from source loopback address [2-441](#)
  - denial of packets from source multicast address [2-441](#)
  - hardware assist [2-311](#)
  - multicast rate limiters [2-513](#)
  - displaying
    - ACL entries [2-1081](#)
    - DSS IP range invalidation profile [2-698](#)
    - DSS IPv6 range invalidation profile [2-698](#)
    - exact route for [2-925](#)
    - FIB TCAM exceptions [2-711](#)
    - hardware NetFlow IPv6 configuration [2-967](#)
    - MFIB information [2-867](#)
    - microflow policing information [2-967](#)
    - MLS IP information [2-940](#)
    - MLS QoS information [2-970](#)
    - multicast entries [2-925](#)
    - multicast hardware shortcut count [2-1033](#)
    - multicast shared adjacencies [2-1033](#)
    - multicast subnet/connected hardware entries [2-1033](#)
    - NetFlow entries [2-957](#)
    - NetFlow hardware configuration [2-957](#)
    - per-prefix accounting statistics [2-925](#)
    - platform software multicast information [2-1033](#)
    - switching table entry information [2-925](#)
  - enabling
    - CEF-based multicast forwarding [2-311](#)
    - compression mode [2-439](#)
    - denial of packets from source loopback address [2-441](#)
    - denial of packets from source multicast address [2-441](#)
    - hardware assist [2-311](#)
  - hardware assist
    - enabling [2-311](#)
  - MLDv2 snooping
    - displaying explicit-tracking information [2-873](#)
    - displaying multicast router interfaces [2-873](#)
    - displaying report-suppression status [2-873](#)
    - displaying statistics information [2-873](#)
  - per-prefix accounting
    - display statistics [2-925](#)
    - preventing
      - installation of ACL entry [2-312](#)
      - installation of multicast connected entry [2-312](#)
  - IPv6 hardware configuration information [2-967](#)
  - IPv6 snooping
    - See MLDv2 snooping
  - IPX (Internet Packet Exchange)
    - access lists, time ranges [2-1227](#)
  - IPX MLS
    - clearing entries [2-73](#)
  - IPX shortcuts to MSFC
    - disabling [2-528](#)
    - enabling [2-528](#)
  - IS-IS
    - configuring network entity title [2-574](#)
  - ISL
    - encapsulation
      - disabling [2-129](#)
      - enabling [2-129](#)
  - ISL VLANs
    - mapping to 802.1Q VLANs [2-1276](#)
- 
- J
- jumbo frames
    - default value [2-569](#)
    - restoring default value [2-569](#)
    - setting maximum packet size [2-569](#)
    - setting maximum transmission unit size [2-569](#)
- 
- L
- LACP
    - configuring
      - maximum port per bundle on port channel [2-342](#)
    - configuring interface [2-22](#)
    - deselecting channeling protocol [2-25](#)

- displaying
    - internal information [2-879](#)
    - neighbor information [2-879](#)
    - protocol setting [2-715](#)
    - statistical information [2-879](#)
    - system identification [2-879](#)
  - setting
    - channeling protocol [2-25](#)
    - ingress packet rate [2-344](#)
    - port priority [2-343](#)
    - system priority [2-345](#)
  - last member query interval
    - configuring for IGMP [2-220](#)
    - configuring for IGMP snooping [2-230](#)
    - configuring for MLDv2 snooping [2-316](#)
  - Layer 2
    - configuring port as a multicast router port [2-233](#)
    - interface type
      - resetting [2-1195](#)
      - setting [2-1195](#)
  - Layer 2 classification of IP packets
    - configuring [2-377](#)
    - disabling [2-379](#)
    - enabling [2-379](#)
  - Layer 2 port-security
    - displaying
      - rate-limiter status information [2-982](#)
      - rate-limiter usage information [2-982](#)
  - Layer 3
    - manager
      - displaying information [2-877](#)
  - Link Aggregation Control Protocol
    - See LACP
  - link debounce timer
    - configuring [2-348](#)
    - disabling [2-348](#)
    - displaying debounce timer configuration [2-753](#)
    - enabling [2-348](#)
  - link-status event messages
    - disabling
      - globally [2-352](#)
      - on an interface [2-354](#)
      - on a subinterface [2-355](#)
      - on system initialization [2-352](#)
    - enabling
      - globally [2-352](#)
      - on an interface [2-354](#)
      - on a subinterface [2-355](#)
      - on system initialization [2-352](#)
  - link type
    - configuring [2-1140](#)
  - load balancing
    - selecting
      - Catalyst 6500 series switch load-balancing algorithm [2-411](#)
      - Cisco IOS load-balancing algorithm [2-411](#)
  - load-balancing algorithm
    - selecting [2-184](#)
  - load statistics interval [2-350](#)
  - logging [2-357](#)
    - controlling IP ARP packets [2-177](#)
  - logical virtual ports
    - displaying number required [2-1112](#)
  - longest prefix match functionality [2-914, 2-929](#)
  - loop guard
    - disabling [2-1139](#)
    - enabling [2-1139](#)
- 
- ## M
- MAC ACL filtering
    - disabling VLAN field [2-379](#)
    - enabling VLAN field [2-379](#)
  - MAC ACL QoS filtering
    - classifying Layer 3 packets as Layer 2 packets [2-377](#)
    - configuring
      - ARP ACL [2-5](#)
    - deleting

- ARP ACL [2-5](#)
- MAC addresses
  - counters
    - displaying multicast addresses [2-884](#)
  - enabling
    - MAC limit globally [2-368](#)
    - MAC limit per interface [2-368](#)
    - MAC limit per port [2-368](#)
    - MAC limit per VLAN [2-368](#)
    - sticky MAC [2-1200](#)
  - removing
    - sticky MAC [2-1200](#)
- MAC address filtering
  - configuring [2-373](#)
  - disabling [2-373](#)
  - enabling [2-373](#)
- MAC address learning
  - disabling [2-366](#)
  - displaying state [2-890](#)
  - enabling [2-366](#)
- MAC address table
  - configuring
    - mac-out-of-band synchronization [2-376](#)
- MAC address tables
  - adding static entries [2-373](#)
  - clearing dynamic entries [2-63](#)
  - clearing static entries [2-63](#)
  - configuring
    - aging time [2-364](#)
    - RM purging time [2-364](#)
  - deleting secure or specific addresses [2-82](#)
  - disabling
    - CAM table usage monitoring notification [2-371](#)
    - IGMP snooping on static MAC addresses [2-373](#)
    - MAC address learning [2-366](#)
    - MAC move notification [2-370](#)
  - displaying
    - aging time [2-884](#)
    - DFC-specific information [2-884](#)
    - dynamic table entries [2-884](#)
    - entry count [2-884](#)
    - information [2-884](#)
    - interface-specific information [2-884](#)
    - MAC address learning state [2-890](#)
    - MAC move notification [2-884](#)
    - multicast table entries only [2-884](#)
    - number of manually configured entries [2-884](#)
    - static table entries only [2-884](#)
    - VLAN-specific information [2-884](#)
  - enabling
    - CAM table usage monitoring notification [2-371](#)
    - MAC address learning [2-366](#)
    - MAC move notification [2-370](#)
  - removing static entries [2-373](#)
- MAC limit
  - disabling [2-368](#)
  - enabling [2-368](#)
- MAC move notification
  - disabling [2-370](#)
  - enabling [2-370](#)
- mac-out-of-band synchronization
  - configuring [2-376](#)
- macro
  - creating an interface-range macro [2-97](#)
- maintenance loop signaling entity
  - See MLSE
- Maintenance Operation Protocol
  - See MOP
- mapping
  - 802.1Q VLANs to ISL VLANs [2-1276](#)
  - accessing
    - QoS policy map configuration mode [2-592](#)
  - configuring
    - DSCP mutation map [2-473](#)
    - egress DSCP-to-CoS mapping [2-470](#)
    - egress DSCP-to-DSCP mapping [2-473](#)
    - egress DSCP-to-EXP mapping [2-472](#)
    - egress EXP-to-EXP mapping [2-476](#)

- EXP mutation map [2-476](#)
- ingress-EXP-to-DSCP mapping [2-475](#)
- ingress IP precedence-to-DSCP mapping [2-478](#)
- policed DSCP values to marked-down DSCP value mapping [2-480](#)
- QoS class maps [2-26](#)
- QoS policy map [2-592](#)
- creating VLAN access map [2-1266](#)
- defining
  - CoS to CoS map [2-468](#)
- deleting
  - CoS-to-DSCP mapping [2-467](#)
  - egress DSCP-to-CoS mapping [2-470](#)
  - egress DSCP-to-DSCP mapping [2-473](#)
  - egress DSCP-to-EXP mapping [2-472](#)
  - egress EXP-to-EXP mapping [2-476](#)
  - ingress-EXP-to-DSCP mapping [2-475](#)
  - ingress IP precedence-to-DSCP mapping [2-478](#)
  - policed DSCP values to marked-down DSCP value mapping [2-480](#)
  - QoS class maps [2-26](#)
  - QoS policy map [2-592](#)
- displaying
  - class map information [2-679](#)
  - information [2-759](#)
  - policy map information [2-1036](#)
  - policy map interface information [2-1040](#)
- entering VLAN access-map command mode [2-1266](#)
- removing VLAN access map [2-1266](#)
- match subcommand
  - accessing [2-26](#)
- maximum NetFlow table allocation
  - configuring [2-452](#)
- maximum routes
  - displaying configuration [2-930](#)
- maximum transmission unit
  - See MTU
- MD5 signature
  - computing [2-1255](#)
- MDIX
  - disabling [2-386](#)
  - enabling [2-386](#)
- MDS
  - disabling
    - IP multicast routing [2-277](#)
  - displaying
    - interface information [2-826](#)
  - enabling
    - IP multicast routing [2-277](#)
- MDSS
  - Multicast Distributed Shortcut Switching
- MDT
  - configuring
    - default group [2-389](#)
    - group address ranges [2-388](#)
  - disabling
    - recording of data MDT reuse [2-390](#)
  - displaying
    - advertisements sent [2-853](#)
    - data reuse information [2-850](#)
    - default group information [2-849](#)
    - detailed BGP advertisement information [2-849](#)
    - hardware accelerated information [2-944](#)
    - received advertisements [2-851](#)
  - enabling
    - recording of data MDT reuse [2-390](#)
- Media Access Control
  - See MAC address table
- media dependent interface with crossover detection
  - See MDIX
- message digest 5
  - See MD5
- message-of-the-day
  - See MOTD
- MFIB
  - displaying entries and interfaces [2-867](#)
- mGRE
  - configuring

- mobility [2-540](#)
- wireless mGRE tunnels [2-540](#)
- specifying
  - convert NBMA to BMA [2-540](#)
  - network ID [2-540](#)
- MIB
  - displaying SNMP interface index identification numbers [2-1062](#)
- microflow policers
  - defining
    - flow mask type [2-587](#)
- microflow policing for bridged traffic
  - enabling [2-460](#)
  - removing [2-460](#)
- microflow policing statistics, displaying [2-960](#)
- minimum links
  - setting [2-601](#)
- MLDv2
  - disabling
    - proxy reporting [2-314](#)
  - displaying
    - explicit-tracking information [2-873](#)
    - MAC-address table information [2-884](#)
    - multicast router interfaces [2-873](#)
    - report-suppression status [2-873](#)
    - statistics information [2-873](#)
- MLDv2 snooping
  - configuring
    - Layer 2 port as a multicast router port [2-320](#)
  - configuring last member query interval [2-316](#)
  - disabling
    - explicit tracking [2-314](#)
    - globally [2-313](#)
    - report suppression [2-322](#)
    - snooping querier [2-321](#)
  - displaying
    - explicit tracking database [2-873](#)
  - enabling
    - explicit tracking [2-314](#)
    - globally [2-313](#)
    - report suppression [2-322](#)
    - snooping querier [2-321](#)
  - limiting size of explicit tracking database [2-318](#)
- MLS
  - CEF
    - displaying CEF table information [2-937](#)
    - displaying information for specific VRF [2-937](#)
  - clearing
    - statistical information [2-78](#)
    - statistical information (deprecated) [2-79](#)
  - configuring
    - fast-aging time [2-397](#)
    - long-aging time [2-398](#)
    - normal-aging time [2-399](#)
    - port-security rate limiters [2-509](#)
    - rate limiters [2-509](#)
  - defining
    - exception priority [2-403](#)
  - directed broadcasts
    - displaying information [2-902](#)
  - disabling
    - Layer 2 protocol-tunneling rate limiters [2-509](#)
    - rate limiters [2-509](#)
  - disabling directed broadcast [2-418](#)
  - displaying
    - ACL merge method [2-733](#)
    - aggregate count of all missed flows [2-988](#)
    - ASIC version [2-896](#)
    - exception priority [2-908](#)
    - last reading of corresponding registers [2-988](#)
    - packet error information [2-986](#)
    - statistical information [2-986](#)
    - statistics data export information [2-980](#)
  - enabling
    - directed broadcast [2-418](#)
    - NetFlow interface-based entry feature [2-451](#)
    - NetFlow protocol-based entry feature [2-451](#)
    - PDU rate limiters [2-509](#)

- rate limiters [2-509](#)
- exception priority
  - defining [2-403](#)
  - displaying information [2-908](#)
- interface
  - assigning a VLAN ID [2-532](#)
  - removing a management interface [2-530](#)
  - removing a VLAN ID [2-532](#)
  - specifying a management interface [2-530](#)
- NDE
  - clearing counters [2-72](#)
  - disabling population of additional fields [2-448](#)
  - displaying status and configuration information [2-980](#)
  - enabling export feature [2-450](#)
  - enabling population of additional fields [2-448](#)
  - removing address [2-531](#)
  - removing filter options [2-446](#)
  - specifying address [2-531](#)
  - specifying filter options [2-446](#)
- permitting traffic [2-420](#)
- QoS
  - disabling ToS to DSCP rewrite [2-490](#)
  - enabling ToS to DSCP rewrite [2-490](#)
  - ToS to DSCP rewrite [2-490](#)
- QoS statistics data export
  - aggregate policer [2-495](#)
  - class map [2-497](#)
  - delimiter [2-499](#)
  - destination address [2-500](#)
  - disabling globally [2-492](#)
  - enabling globally [2-492](#)
  - interval [2-502](#)
  - per-port disabling [2-493](#)
  - per-port enabling [2-493](#)
- rate limiters
  - displaying information [2-982](#)
  - displaying Layer 2 port-security information [2-982](#)
  - enabling [2-520](#)
  - enabling CEF rate limiters [2-518](#)
  - enabling for ACL-bridged rate limiters [2-516](#)
  - enabling for Layer 3 security rate limiters [2-523](#)
  - enabling for unicast and multicast packets [2-508](#)
  - enabling for VACL-log cases [2-524](#)
  - setting [2-508](#)
  - setting CEF rate limiters [2-518](#)
  - setting for ACL-bridged rate limiters [2-516](#)
  - setting for Layer 3 security rate limiters [2-523](#)
  - setting for unicast packets [2-520](#)
  - setting for VACL-log cases [2-524](#)
- removing excluded protocol port [2-405](#)
- restoring flow mask [2-407](#)
- selecting ACL merge method [2-393](#)
- specifying excluded protocol port [2-405](#)
- specifying flow mask [2-407](#)
- TCL
  - displaying information [2-988](#)
- VLAN
  - displaying statistical information [2-998](#)
- VTP domain
  - linking [2-533](#)
  - removing [2-533](#)
- MLS CEF
  - displaying
    - consistency checker information [2-912](#)
- MLS IP
  - clearing
    - entries [2-73](#)
    - software-installed entries [2-73](#)
  - configuring
    - OAL globally [2-357](#)
    - OAL on an interface [2-359](#)
  - deleting
    - ACL threshold [2-417](#)
  - disabling
    - ACL logical operations expansion on Layer 4 ports [2-409](#)
    - egress replication mode [2-431](#)
    - ingress replication mode [2-431](#)

- OAL globally [2-357](#)
- OAL on an interface [2-359](#)
- shortcuts in TCAM [2-438](#)
- displaying
  - information [2-940](#)
  - mode information [2-944](#)
  - multicast replication capabilities [2-944](#)
  - NetFlow routing entries [2-952](#)
  - OAL-cache entries [2-882](#)
  - OAL configuration information [2-882](#)
  - PIM group to active rendezvous point mappings [2-948](#)
  - software-installed non-static entry information [2-951](#)
  - software-installed static entry information [2-954](#)
  - statistical information for NetFlow entries [2-955](#)
- enabling
  - ACL logical operations expansion on Layer 4 ports [2-409](#)
  - egress replication mode [2-431](#)
  - ingress replication mode [2-431](#)
  - OAL globally [2-357](#)
  - OAL on an interface [2-359](#)
  - shortcuts in TCAM [2-438](#)
- global
  - configuring Bidir RP RPF scan interval [2-425](#)
  - configuring threshold [2-435](#)
  - disabling [2-422](#)
  - disabling consistency checker [2-428](#)
  - disabling subnet download [2-426](#)
  - disabling support for policy-routed packets [2-437](#)
  - enabling [2-422](#)
  - enabling consistency checker [2-428](#)
  - enabling subnet download [2-426](#)
  - enabling support for policy-routed packets [2-437](#)
- installing
  - ACL threshold [2-421](#)
- interface
  - disabling external switches [2-527](#)
  - disabling internal router [2-408](#)
  - disabling shortcuts [2-424](#)
  - enabling external switches [2-527](#)
  - enabling internal router [2-408](#)
  - enabling non-RPF multicast fastdrop [2-433](#)
  - enabling shortcuts [2-424](#)
- IP shortcuts to MSFC
  - disabling [2-526](#)
  - enabling [2-526](#)
- multicast
  - enabling egress capability [2-422](#)
- reflexive NDR
  - disabling shortcuts in TCAM [2-438](#)
  - enabling shortcuts in TCAM [2-438](#)
- replication mode
  - disabling egress mode [2-431](#)
  - disabling ingress mode [2-431](#)
  - enabling egress mode [2-431](#)
  - enabling ingress mode [2-431](#)
- MLS IPX
  - interface
    - disabling external switches [2-529](#)
    - enabling external switches [2-529](#)
  - IPX shortcuts to MSFC
    - disabling [2-528](#)
    - enabling [2-528](#)
- MLS per-prefix accounting
  - disabling [2-410](#)
  - enabling [2-410](#)
- MLS QoS
  - aggregate policer
    - clearing statistics and token counts in high-rate and low-rate policer buckets [2-76](#)
    - defining [2-458](#)
    - removing [2-458](#)
  - attaching
    - CoS mutation map to interface [2-463](#)
    - DSCP mutation map to interface [2-464](#)
    - EXP mutation map to interface [2-465](#)
  - attaching a policy map to an interface [2-647](#)

- clearing statistics and token counts in high-rate and low-rate policer buckets [2-76](#)
- default CoS value
  - defining [2-462](#)
  - removing [2-462](#)
- defining
  - ingress-EXP-to-DSCP mapping [2-475](#)
- disabling
  - policer traffic class identification [2-483](#)
  - policing ACL-redirected packets [2-485](#)
  - port attribute checks on EtherChannel bundling [2-461](#)
  - port queueing mode [2-488](#)
  - port-trust ignore [2-482](#)
- displaying
  - information [2-970](#)
  - IPv6 information [2-970](#)
  - map configuration information [2-975](#)
  - MPLS interface summary [2-977](#)
  - number of free aggregate RAM indexes on the switch processor and the DFCs [2-974](#)
  - runtime version information [2-975](#)
- DSCP mutation mapping
  - defining [2-473](#)
  - removing [2-473](#)
- egress DSCP-to-CoS mapping
  - defining [2-470](#)
  - deleting [2-470](#)
- egress DSCP-to-EXP mapping
  - defining [2-472](#)
  - deleting [2-472](#)
- enabling
  - policer traffic class identification [2-483](#)
  - policing ACL-redirected packets [2-485](#)
  - port attribute checks on EtherChannel bundling [2-461](#)
  - port queueing mode [2-488](#)
  - port-trust ignore [2-482](#)
- EXP mutation mapping
  - defining [2-476](#)
  - removing [2-476](#)
- extended trust
  - configuring trust mode [2-505](#)
  - displaying trust mode [2-1051](#)
- global
  - disabling [2-455](#)
  - disabling PFC QoS and enabling port queueing [2-455](#)
  - enabling [2-455](#)
- ingress CoS-to-DSCP mapping
  - defining [2-467](#)
  - removing [2-467](#)
- ingress-EXP-to-DSCP mapping
  - defining [2-475](#)
  - deleting [2-475](#)
- ingress IP precedence-to-DSCP mapping
  - defining [2-478](#)
  - removing [2-478](#)
- interface
  - changing to untrusted port state [2-484, 2-503](#)
  - disabling [2-457](#)
  - enabling [2-457](#)
  - setting trusted port state [2-484, 2-503](#)
- mapping
  - defining CoS to CoS map [2-468](#)
- microflow policing for bridged traffic
  - enabling [2-460](#)
  - removing [2-460](#)
- MPLS
  - displaying interface summary [2-977](#)
- policed in-profile DSCP mapping
  - defining [2-480](#)
  - removing [2-480](#)
- policing
  - ACL-redirected packets [2-485](#)
- policy-map configuration mode
  - accessing [2-592](#)
  - exiting [2-592](#)
- removing
  - CoS mutation map from interface [2-463](#)
  - DSCP mutation map from interface [2-464](#)

- EXP mutation map from interface [2-465](#)
- removing a policy map from an interface [2-647](#)
- VLAN switch port
  - disabling [2-507](#)
  - enabling [2-507](#)
- MLS QoS policy maps
  - class option description, table [2-587, 2-593](#)
  - configuring [2-592](#)
- MMLS
  - displaying
    - explicit tracking information [2-990](#)
    - information [2-991](#)
- mobility [2-540](#)
- modes
  - See command modes
- modules
  - disabling
    - oversubscription mode [2-151](#)
  - displaying
    - provisioning information [2-998](#)
    - status information [2-998](#)
    - version information [2-998](#)
  - enabling
    - oversubscription mode [2-151](#)
  - power cycling [2-152](#)
  - powering down [2-603](#)
  - powering on [2-603](#)
  - shutdown NAM [2-153](#)
  - shutdown SSL [2-153](#)
  - specifying
    - boot options [2-149](#)
- MOP (Maintenance Operation Protocol)
  - server
    - booting automatically [2-15](#)
- more commands
  - filter [1-7](#)
  - search [1-7](#)
- More-- prompt [1-7](#)
  - filter [1-7](#)
- search [1-7](#)
- MPLS
  - clearing
    - software-installed entries [2-73](#)
  - configuring
    - burst duration for GB-TE flows [2-444](#)
    - global parameters [2-444](#)
  - configuring DSCP map for GB-TE flows [2-444](#)
  - defining
    - DSCP-to-EXP mapping [2-472](#)
  - deleting
    - DSCP-to-EXP map [2-472](#)
  - disabling
    - aggregated label recirculation [2-444](#)
    - recirculation [2-442](#)
    - tag-to-tag load balancing [2-567](#)
    - tunnel recirculation [2-444](#)
  - disabling routing [2-565](#)
  - displaying
    - control plane statistics [2-1010](#)
    - FIB TCAM exceptions [2-711](#)
    - information [2-940](#)
    - interface summary [2-977](#)
    - IoMPLS enabled interface information [2-1010](#)
    - platform-specific information [2-1010](#)
    - shared code between LAN and WAN [2-1010](#)
    - state of currently routed VCs [2-1006](#)
    - VPN to VLAN mapping table [2-1010](#)
  - enabling
    - aggregated label recirculation [2-444](#)
    - recirculation [2-442](#)
    - tag-to-tag load balancing [2-567](#)
    - tunnel recirculation [2-444](#)
  - enabling routing [2-565](#)
  - load distribution method
    - resetting to defaults [2-599](#)
    - setting [2-599](#)
  - setting
    - experimental value [2-657](#)

- redundancy mode [2-542](#)
  - trusted state on Layer 2 WAN interface [2-658](#)
- specifying
  - use optimized MPLS tagging [2-568](#)
  - use standard MPLS tagging [2-568](#)
- tagging
  - specify using optimized tagging [2-568](#)
  - specify using standard tagging [2-568](#)
- tag switching
  - disabling load balancing [2-567](#)
  - displaying table information [2-1013](#)
  - enabling load balancing [2-567](#)
- MPLS EXP
  - MPLS experimental field
    - See MPLS
- mroute
  - configuring
    - static route [2-243](#)
- MSDP
  - adding
    - descriptive text to configuration [2-250](#)
  - bringing up the peer [2-265](#)
  - clearing
    - SA-cache entries [2-55](#)
    - statistics counters [2-56](#)
    - TCP connection to the MSDP peer [2-54](#)
  - configuring
    - entries advertised in SA messages [2-257](#)
    - for PIM sparse mode region [2-245](#)
    - incoming filter list [2-259](#)
    - originator identification [2-254](#)
    - outgoing filter list [2-261](#)
    - peers [2-255](#)
    - peer to mesh group [2-253](#)
    - router to send SA request messages [2-263](#)
    - router to send SA requests [2-251](#)
  - creating
    - SA state [2-247](#)
  - defining
    - default peer [2-248](#)
  - displaying
    - number of sources and groups [2-836](#)
    - peer information [2-838](#)
    - states learned from MSDP peers [2-840](#)
  - displaying peer status [2-842](#)
  - enabling
    - administrative shut down of peer [2-265](#)
  - limiting
    - multicast data packets [2-266](#)
  - removing
    - incoming filter list [2-259](#)
    - outgoing filter list [2-261](#)
    - peers [2-255](#)
    - removing peer from mesh group [2-253](#)
- MSFC
  - displaying
    - standby MSFC2 DRAM [2-668](#)
  - programing new ROMMON into Flash [2-1252](#)
  - setting execution preference [2-1252](#)
- MST
  - configuration submode command
    - instance [2-155](#)
    - name [2-571](#)
    - revision [2-637](#)
    - show [2-659](#)
  - configuring
    - forward delay [2-1147](#)
    - hello-time [2-1148](#)
    - max-age [2-1149](#)
    - max-hops [2-1150](#)
    - port to transmit prestandard BPDUs [2-1151](#)
    - root as primary [2-1153](#)
    - root as secondary [2-1153](#)
  - displaying
    - current configuration [2-659](#)
    - MST protocol information [2-1070](#)
    - MST region configuration information [2-1070](#)
    - pending configuration [2-659](#)

- entering configuration submode [2-1145](#)
- instance
  - mapping VLANs [2-155](#)
- mapping
  - PVLANS to instance [2-614](#)
  - VLANs [2-155](#)
- restarting protocol migration [2-84](#)
- setting
  - configuration revision number [2-637](#)
  - MST region name [2-571](#)
  - path cost for instances [2-1143](#)
  - port priority for instances [2-1143](#)
  - switching to PVST mode [2-1142](#)
- MTU
  - default values [2-569](#)
  - displaying global MTU settings [2-1078](#)
  - displaying system MTU setting [2-1078](#)
  - restoring default value [2-569](#)
  - setting
    - maximum Layer 2 payload size [2-1221](#)
    - maximum Layer 3 payload size [2-1221](#)
    - maximum packet size [2-569](#)
    - maximum size [2-569](#)
- multicast distributed switching
  - See MDS
- multicast distribution tree
  - See MDT
- multicast forwarding information base
  - See MFIB
- multicast router
  - displaying routing table [2-829, 2-834](#)
  - displaying snooping information [2-815](#)
- multicast SSO
  - configuring
    - leak interval [2-432](#)
    - leak percentage [2-432](#)
  - configuring convergence timer [2-432](#)
  - displaying
    - information [2-949](#)
    - statistical information [2-949](#)
- multicast static route
  - See mroute
- Multilayer Switching
  - See MLS
- multiple-character patterns [1-9](#)
- multiple NetFlow export destinations, configuring [2-207](#)
- multiple path unicast RPF check
  - configuring
    - modes [2-416](#)
  - creating
    - interface group [2-415](#)
  - deleting
    - interface group [2-415](#)
  - interface group
    - creating [2-415](#)
    - defining [2-415](#)
    - deleting [2-415](#)
  - RPF mode
    - interface-group [2-416](#)
    - pass [2-416](#)
    - punt [2-416](#)
- Multiple Spanning Tree
  - See MST
- multipoint generic routing encapsulation
  - See mGRE
- Multiprotocol Label Switching
  - See MPLS
- mVPN
  - adding
    - descriptive text to MSDP configuration [2-250](#)
  - allocating circular buffer storage [2-269](#)
  - bringing up the MSDP peer [2-265](#)
  - clearing
    - SA-cache entries [2-55](#)
    - statistics counters [2-56](#)
    - TCP connection to the MSDP peer [2-54](#)
  - configuring
    - advertising to the BSR [2-291](#)

- BSR candidacy [2-286](#)
  - default group [2-389](#)
  - entries advertised in SA messages [2-257](#)
  - incoming filter list [2-259](#)
  - originator identification [2-254](#)
  - outgoing filter list [2-261](#)
  - peers [2-255](#)
  - peer to mesh group [2-253](#)
  - PIM message acceptance [2-282](#)
  - PIM sparse mode region for MSDP [2-245](#)
  - register source [2-289](#)
  - rendezvous point mapping agent [2-295](#)
  - router to send SA request messages [2-263](#)
  - router to send SA requests [2-251](#)
  - shortest path tree, delaying use [2-299](#)
  - using Auto-RP [2-293](#)
  - creating
    - SA state [2-247](#)
  - defining
    - default peer [2-248](#)
    - SSM range of IP multicast addresses [2-300](#)
  - deleting
    - Auto-RP cache entries [2-57](#)
    - entries from IGMP-group cache [2-49](#)
    - entries from IP multicast routing table [2-52](#)
  - disabling
    - bidir-PIM [2-284](#)
    - IP multicast routing [2-277](#)
    - load splitting across multiple paths [2-274](#)
    - SSM range of IP multicast addresses [2-300](#)
  - displaying
    - BSR information [2-846](#)
    - cached rendezvous points [2-858](#)
    - contents of circular cache-header buffer [2-827](#)
    - contents of IP fast-switching cache [2-824](#)
    - data MDT reuse information [2-850](#)
    - designated forwarder interface information [2-848](#)
    - detailed BGP advertisement information [2-849](#)
    - discovered neighbors [2-854](#)
    - MDT interface information [2-826](#)
    - MDT advertisement sent [2-853](#)
    - MSDP peer status [2-842](#)
    - number of sources and groups [2-836](#)
    - peer information [2-838](#)
    - received MDT advertisements [2-851](#)
    - rendezvous points for a group [2-856](#)
    - states learned from MSDP peers [2-840](#)
    - triggered RPF check events [2-864](#)
  - enabling
    - administrative shut down of peer [2-265](#)
    - bidir-PIM [2-284](#)
    - IP multicast routing [2-277](#)
    - load splitting across multiple paths [2-274](#)
  - filtering
    - Auto-RP messages [2-290](#)
    - multicast router information request packets [2-273](#)
    - filtering PIM register messages [2-281](#)
  - limiting
    - multicast data packets [2-266](#)
  - limiting number of routes added to table [2-276](#)
  - removing
    - Auto-RP message filter [2-290](#)
    - circular buffer [2-269](#)
    - incoming filter list [2-259](#)
    - outgoing filter list [2-261](#)
    - peers [2-255](#)
  - removing peer from mesh group [2-253](#)
  - setting
    - register message limit [2-288](#)
- 
- ## N
- ### NDE
- clearing
    - counters [2-72](#)
  - disabling
    - population of additional fields [2-448](#)
    - sampled NetFlow on an interface [2-453](#)

- displaying
  - aging information [2-957](#)
  - hardware status [2-957](#)
  - sampled NetFlow status [2-985](#)
  - status and configuration information [2-980](#)
  - status information [2-956](#)
- enabling
  - export feature [2-450](#)
  - population of additional fields [2-448](#)
  - sampled NetFlow on an interface [2-453](#)
- filter options
  - removing [2-446](#)
  - specifying [2-446](#)
- removing address [2-531](#)
- sampled NetFlow
  - disabling on an interface [2-453](#)
  - enabling on an interface [2-453](#)
  - specifying sampling method [2-534](#)
- specifying address [2-531](#)
- NDE interface export
  - flow masks [2-446](#)
  - specifying filter options [2-446](#)
- NET
  - configuring [2-574](#)
- NetFlow
  - aggregation
    - configuring specific aggregation caches [2-202](#)
    - displaying cache flow entries [2-785](#)
  - clearing counters [2-37](#)
  - configuring
    - aggregation caches—specific [2-202](#)
    - maximum flow allocation [2-452](#)
    - multiple export destination [2-207](#)
  - disabling
    - globally for bridged flows [2-216](#)
    - inbound NDE for bridged flows [2-215](#)
    - interface-based NDE [2-210](#)
    - multicast ingress accounting [2-275](#)
    - NDE for hardware-switched flows [2-206](#)
  - sampled NetFlow globally [2-534](#)
  - displaying [2-967](#)
    - aging information [2-957](#)
    - cache flow entries [2-785](#)
    - detailed statistics summary [2-789](#)
    - fragment offset information [2-789](#)
    - hardware status [2-957](#)
    - IP flow information [2-960](#)
    - IP flow mask [2-957](#)
    - IP information [2-957](#)
    - microflow policing statistics [2-960](#)
    - software-installed non-static entry information [2-965](#)
    - statistical information [2-940](#)
    - switched packet counts [2-986](#)
    - table information [2-940](#)
  - enabling
    - globally for bridged flows [2-216](#)
    - inbound NDE for bridged flows [2-215](#)
    - interface-based entry creation [2-451](#)
    - interface-based NDE [2-210](#)
    - multicast ingress accounting [2-275](#)
    - NDE for hardware-switched flows [2-206](#)
    - protocol-based entry creation [2-451](#)
    - sampled NetFlow globally [2-534](#)
    - switching [2-304](#)
  - hardware switching
    - disabling interface-based entry creation [2-451](#)
    - disabling protocol-based entry creation [2-451](#)
    - displaying CEF table information [2-797](#)
    - enabling interface-based entry creation [2-451](#)
    - enabling protocol-based entry creation [2-451](#)
  - incorporating bridged/IntraVLAN traffic [2-460](#)
  - interface
    - specifying source interface [2-211](#)
  - interface-based NDE
    - disabling [2-210](#)
    - enabling [2-210](#)
  - IPv6
    - displaying hardware configuration information [2-967](#)

- monitoring
    - NetFlow table usage on switch processor [2-454](#)
  - software switching
    - displaying information [2-807](#)
  - specifying
    - export flow version on Supervisor Engine 720 [2-213](#)
    - hardware-switched flow NDE version [2-209](#)
  - switching
    - clearing statistics [2-48](#)
    - displaying cache flow entries [2-785](#)
    - exporting cache entries [2-207](#)
    - setting cache size [2-204](#)
    - specifying source interface [2-211](#)
  - table usage on switch processor
    - monitoring [2-454](#)
  - NetFlow Data Export
    - See NDE
  - net processor
    - displaying
      - counter information [2-1026](#)
  - network entity title
    - See NET
  - next-hop
    - displaying CEF VLAN information [2-798](#)
  - Next Hop Resolution Protocol
    - See NHRP
  - NHRP
    - displaying
      - cache [2-843](#)
  - nodal NSF, configuring [2-642](#)
  - no form of a command, using [1-7](#)
  - non-RPF multicast fastdrop
    - enabling [2-433](#)
  - non-stop forwarding
    - See NSF
  - non-XL mode
    - definition
      - support modules [2-401](#)
  - NSF
    - cancelling OSPF restart [2-576](#)
    - disabling [2-576](#)
      - BGP routing process [2-644](#)
      - EIGRP routing process [2-644](#)
      - IS-IS routing process [2-644](#)
      - OSPF routing process [2-644](#)
    - enabling
      - BGP routing process [2-644](#)
      - EIGRP routing process [2-644](#)
      - IS-IS routing process [2-644](#)
      - OSPF routing process [2-644](#)
    - specifying
      - Cisco proprietary IS-IS method [2-576](#)
      - failover interval [2-576](#)
      - IETF IS-IS method [2-576](#)
      - IS-IS database synchronization wait time [2-576](#)
      - route processor stabilizer interval [2-576](#)
- 
- O
  - OAL
    - clearing entries [2-62](#)
    - configuring
      - global [2-357](#)
      - interface [2-359](#)
    - displaying
      - cache entries [2-882](#)
      - configuration information [2-882](#)
  - ODM
    - selecting ACL merge method [2-393](#)
  - ondemand diagnostics
    - configuring [2-107](#)
      - execution action for test failure [2-107](#)
  - online diagnostics
    - bypassing boot-up diagnostic testing [2-99](#)
    - configuring
      - execution action for test failure [2-107](#)
      - health monitoring diagnostic tests [2-104](#)
      - ondemand diagnostics [2-107](#)

- disabling
    - publishing to CNS event bus [2-101](#)
    - subscription to CNS diagnostic events [2-101](#)
  - displaying
    - CNS subject [2-688](#)
    - configured boot-up coverage level [2-683](#)
    - current scheduled tasks [2-683](#)
    - event logs [2-683](#)
    - sanity check results [2-689](#)
    - supported test suites [2-683](#)
    - test ID [2-683](#)
    - test results [2-683](#)
    - test statistics [2-683](#)
  - enabling
    - publishing to CNS event bus [2-101](#)
    - scheduling [2-108](#)
    - subscription to CNS diagnostic events [2-101](#)
    - syslog messages [2-104](#)
  - global configuration mode
    - clearing health monitoring diagnostic test schedule [2-104](#)
    - clearing schedule [2-99](#)
    - clearing test-based testing schedule [2-108](#)
    - setting boot-up diagnostic level [2-99](#)
    - setting health monitoring diagnostic testing [2-104](#)
    - setting test-based testing [2-108](#)
    - setting up health monitoring diagnostic test schedule [2-104](#)
    - setting up schedule [2-99](#)
    - setting up test-based testing [2-108](#)
  - removing
    - scheduling [2-108](#)
  - returning to default setting [2-99](#)
  - scheduled switchover
    - disabling [2-108](#)
    - enabling [2-108](#)
  - setting
    - testing level [2-99](#)
    - test interval [2-108](#)
  - specifying
    - health monitoring diagnostic tests [2-104](#)
    - starting testing [2-111, 2-113](#)
  - optimized ACL logging
    - See OAL
  - order-dependent merge algorithm
    - See ODD
  - OSPF
    - specifying
      - minimum percentage of CPU process time [2-615](#)
- 
- P
- packet buffer errors
    - displaying status [2-712, 2-713](#)
    - enabling error detection [2-132](#)
  - packet count, displaying [2-750](#)
  - packet error information, displaying [2-986](#)
  - paging prompt
    - see --More-- prompt
  - PAgP
    - clearing information [2-80](#)
    - configuring interface [2-22](#)
    - deselecting channeling protocol [2-25](#)
    - displaying
      - protocol information [2-715](#)
    - hot standby mode
      - returning to defaults [2-580](#)
      - selecting ports [2-580](#)
    - input interface of incoming packets
      - learning [2-579](#)
      - returning to defaults [2-579](#)
    - port channels
      - displaying information [2-1014](#)
    - setting
      - channeling protocol [2-25](#)
  - passwords
    - establishing enhanced password security [2-1254](#)
    - setting username [2-1254](#)

- pathcost
  - setting STP default pathcost calculation method [2-1155](#)
- PBR
  - disabling [2-437](#)
  - enabling [2-437](#)
    - hardware support for null0 route maps
- per-prefix accounting
  - disabling [2-410](#)
  - enabling [2-410](#)
- per VLAN learning [A-7](#)
- per-VLAN spanning tree
  - See PVST+
- PIM
  - clearing
    - global statistical information [2-58](#)
    - statistical VLAN information [2-59](#)
  - configuring
    - advertising to the BSR [2-291](#)
    - BSR candidacy [2-286](#)
    - message acceptance [2-282](#)
    - PIM sparse mode region for MSDP [2-245](#)
    - register source [2-289](#)
    - rendezvous point mapping agent [2-295](#)
    - shortest path tree, delaying use [2-299](#)
    - using Auto-RP [2-293](#)
  - defining
    - SSM range of IP multicast addresses [2-300](#)
  - deleting
    - Auto-RP cache entries [2-57](#)
  - disabling
    - bidir-PIM [2-284](#)
    - flooding of packets to designated router [2-298](#)
    - processing and forwarding of PIM dense mode state refresh control messages [2-301](#)
    - snooping globally [2-296](#)
    - snooping on an interface [2-297](#)
    - SSM range of IP multicast addresses [2-300](#)
    - triggered RPF check [2-278](#)
  - displaying
    - BSR information [2-846](#)
    - cached rendezvous points [2-858](#)
    - data MDT reuse information [2-850](#)
    - designated forwarder interface information [2-848](#)
    - detailed BGP advertisement information [2-849](#)
    - discovered neighbors [2-854](#)
    - IP multicast routing table information [2-834](#)
    - MDT advertisement sent [2-853](#)
    - PIM group to active rendezvous point mappings [2-948](#)
    - received MDT advertisements [2-851](#)
    - rendezvous points for a group [2-856](#)
    - snooping information [2-860](#)
    - triggered RPF check events [2-864](#)
  - enabling
    - bidir-PIM [2-284](#)
    - flooding of packets to designated router [2-298](#)
    - processing and forwarding of PIM dense mode state refresh control messages [2-301](#)
    - snooping globally [2-296](#)
    - snooping on an interface [2-297](#)
  - filtering
    - Auto-RP messages [2-290](#)
  - filtering register messages [2-281](#)
  - removing
    - Auto-RP message filter [2-290](#)
  - setting
    - back-off interval [2-278](#)
    - check interval [2-280](#)
    - register message limit [2-288](#)
    - triggered check interval [2-278](#)
  - snooping
    - clearing global statistical information [2-58](#)
    - clearing statistical VLAN information [2-59](#)
    - disabling globally [2-296](#)
    - disabling on an interface [2-297](#)
    - enabling globally [2-296](#)
    - enabling on an interface [2-297](#)
- pipe symbol

- specifying alternative patterns [1-10](#)
- PIR
  - setting peak rate
- PISA
  - displaying
    - counter information [2-1026](#)
- platform
  - clearing
    - interrupt throttling counters [2-81](#)
  - displaying
    - CPU EEPROM information [2-1016](#)
    - fault data [2-1016](#)
    - interrupt throttling information [2-1016](#)
    - IP multicast-related information [2-1016](#)
    - MSFC information [2-1016](#)
    - net interrupt information [2-1016](#)
    - processor TLB register information [2-1016](#)
- platforms
  - displaying
    - buffer allocation information [2-1016](#)
    - hardware resources [2-1020](#)
- point-to-point link type
  - configuring [2-1140](#)
- policer
  - See aggregate policer
- policers
  - defining
    - flow mask type [2-587](#)
    - microflow policers [2-587](#)
  - microflow
    - defining [2-587](#)
    - removing [2-587](#)
  - removing
    - microflow policers [2-587](#)
  - removing aggregate policer from current class [2-587](#)
  - specifying
    - aggregate policer for current class [2-587](#)
- policy-based routing
  - See PBR
- policy maps
  - clearing marking configuration [2-653](#)
  - defining aggregate policer
  - displaying information [2-1036](#)
  - displaying per-interface information [2-1040](#)
  - marking matched traffic with DSCP value [2-653](#)
  - marking matched traffic with IP precedence value [2-655](#)
- port access maps
  - creating [2-595](#)
  - deleting [2-595](#)
- port channels
  - accessing [2-160](#)
  - clearing information [2-80](#)
  - creating [2-160](#)
  - displaying
    - channel group information [2-1014](#)
    - counter information [2-750](#)
    - interface capabilities [2-747](#)
- load distribution method
  - resetting to default [2-602](#)
  - resetting to defaults for bundled ports [2-597](#)
  - setting for bundled ports [2-597](#)
  - setting for specific modules [2-597](#)
  - setting on a per-module basis [2-602](#)
- setting
  - load distribution method for MPLS packets [2-599](#)
  - minimum links [2-601](#)
- port-clocking mode
  - active mode [2-88](#)
  - automatic mode [2-88](#)
  - enabling [2-88](#)
  - passive mode [2-88](#)
- portName MIB objects
  - configuring [2-1172](#)
- port permit list
  - displaying destination list [2-1001](#)
- port ranges
  - executing [2-162](#)
- port security

- configuring [2-134](#)
  - aging time [2-1198](#)
  - aging type [2-1198](#)
- deleting secure or specific addresses [2-82](#)
- disabling [2-1197](#)
- displaying setting information [2-1042](#)
- enabling [2-1197](#)
- removing
  - MAC address from list [2-1200](#)
- setting
  - maximum number of secured addresses [2-1202](#)
  - violation action [2-1204](#)
  - violation actions [2-1204](#)
- port speeds
  - configuring [2-1168](#)
  - default [2-1168](#)
- port-trust ignore
  - disabling [2-482](#)
  - enabling [2-482](#)
- power cycling modules [2-152](#)
- powering down empty slots [2-603](#)
- power redundancy mode
  - setting [2-605](#)
- power status
  - displaying [2-1044](#)
- power supplies
  - displaying
    - product number [2-739](#)
    - serial number [2-739](#)
    - type [2-739](#)
  - setting power redundancy mode [2-605](#)
- private VLANs
  - See PVLANS
- privileged EXEC mode, summary [1-6](#)
- Programmable Intelligent Services Accelerator
  - See PISA
- promiscuous ports
  - setting mode [2-1195](#)
- prompts
  - system [1-6](#)
- Protocol Independent Multicast
  - See PIM
- protocol tunneling
  - disabling interfaces [2-333](#)
  - displaying protocols [2-875](#)
  - enabling interfaces [2-333](#)
  - setting
    - CoS value [2-335](#)
    - drop threshold globally [2-338](#)
    - drop threshold on an interface [2-336](#)
    - specifying maximum processed protocol packets [2-339](#)
- protocol tunneling links
  - converting PVST+ and 802.1d BPDUs [2-18](#)
- proxy reporting
  - disabling [2-224, 2-314](#)
  - enabling
    - turned on by default [2-224, 2-314](#)
- psecure
  - See port security
- PVL
  - disabling [2-366](#)
  - enabling [2-366](#)
- PVLANS [2-1107](#)
  - defining association [2-1206](#)
  - deleting association [2-1206](#)
  - disabling
    - global sticky ARP [2-306](#)
    - per-interface sticky ARP [2-308](#)
  - displaying
    - configuration information [2-764, 2-766](#)
    - currently configured information [2-1107, 2-1112](#)
    - mapping information [2-759](#)
  - enabling
    - global sticky ARP [2-306](#)
    - per-interface sticky ARP [2-308](#)
  - mapping
    - for promiscuous port [2-1207](#)
    - primary and secondary VLAN [2-612](#)

- to an instance [2-614](#)
- setting
  - host ports [2-1195](#)
  - interface type [2-1195](#)
  - promiscuous mode [2-1195](#)
- VLAN interface configuration mode
  - mapping [2-612](#)
  - primary and secondary VLAN mapping [2-612](#)
  - removing mappings [2-612](#)
- VLAN submode
  - adding VLANs [2-609](#)
  - configuring association [2-609](#)
  - designating VLANs [2-609](#)
  - removing VLANs [2-609](#)
- PVST
  - switching to MST mode [2-1142](#)
- PVST+ BPDU and 802.1d BPDU conversion over protocol tunneling links [2-18](#)
- PVST and PVST+ interoperability
  - ignore-bpdu-pid keyword [2-18](#)
  - L2PT topologies [2-19](#)

---

## Q

### QDM

- disconnecting a session [2-114](#)
- displaying
  - client ID [2-1048](#)
  - information and status about currently active QDM clients [2-1048](#)

### QinQ

- creating
  - link bundle (port-channel) virtual interface [2-160](#)
- disabling
  - double-tagged VLAN translation
- enabling
  - double-tagged VLAN translation
- IEEE 802.1Q in 802.1Q
  - See 802.1Q tunneling

- removing
  - link bundle (port-channel) virtual interface [2-160](#)
- setting
  - prioritization bits [2-651](#)

### QM

- displaying switch processor information [2-1049](#)

### QoS

- accessing
  - class map configuration mode [2-26](#)
- avoidance of routing protocol packet policing [2-486](#)
- class map
  - displaying information [2-679](#)
- clearing FM NetFlow counters [2-37](#)
- clearing global interface counters [2-35](#)
- configuring
  - class maps [2-26](#)
  - queueing mode [2-489](#)
  - time-based ACLs [2-1227](#)
- control of routing protocol packet policing [2-486](#)
- defining
  - marking [2-486](#)
- displaying
  - protocol [2-979](#)
- enabling
  - time-based ACLs [2-1227](#)
- manager
  - displaying information [2-1049](#)
- policy maps
  - clearing marking configuration [2-653](#)
  - displaying information [2-1036](#)
  - displaying per-interface information [2-1040](#)
  - marking matched traffic with DSCP value [2-653](#)
  - marking matched traffic with IP precedence value [2-655](#)
- queueing mode [2-489](#)
- rcv-queue ratio limit
  - setting [2-620](#)
- removing
  - ACL time-range limitation [2-1227](#)

- transmit-queue size ratio
  - setting [2-1287](#)
- QoS Device Manager
  - See QDM
- QoS filtering
  - enabling
    - DSCP-based egress [2-581](#)
    - IP precedence based [2-581](#)
- QoS statistics data export
  - See MLS QoS statistics data export
- question command [1-2](#)
- queueing
  - displaying information [2-1051](#)

---

## R

- rapid per-VLAN spanning tree
  - See rapid PVST
- rapid PVST
  - disabling [2-1142](#)
  - enabling [2-1142](#)
- Rapid Spanning Tree Protocol
  - See RSTP
- Rapid Spanning Tree Protocol+
  - See RSTP+
- rate limiters
  - configuring
    - IPv4 multicast rate limiters [2-511](#)
    - IPv6 multicast rate limiters [2-513](#)
    - Layer 2 protocol-tunneling rate limiters [2-509](#)
    - PDU rate limiters [2-509](#)
    - port-security rate limiters [2-509](#)
  - disabling
    - CEF rate limiters [2-518](#)
    - IPv4 multicast rate limiters [2-511](#)
    - IPv6 multicast rate limiters [2-513](#)
    - Layer 2 protocol-tunneling rate limiters [2-509](#)
    - Layer 3 security rate limiters for unicast packets [2-523](#)
  - enabling
    - Layer 2 protocol-tunneling rate limiters [2-509](#)
    - Layer 3 security rate limiters for unicast packets [2-523](#)
    - PDU rate limiters [2-509](#)
    - port-security rate limiters [2-509](#)
  - enabling for ACL-bridged rate limiters [2-516](#)
  - enabling for unicast and multicast packets [2-508](#)
  - enabling for unicast packets [2-520](#)
  - enabling for VACL-log cases [2-524](#)
- MLS
  - displaying
    - Layer 2 port-security information [2-982](#)
  - MLS unicast
    - displaying information [2-982](#)
  - multicast
    - displaying information [2-982](#)
  - setting
    - Layer 3 security rate limiters for unicast packets [2-523](#)
    - setting for ACL-bridged rate limiters [2-516](#)
    - setting for CEF rate limiters [2-518](#)
    - setting for unicast packets [2-508, 2-520](#)
    - setting for VACL-log cases [2-524](#)
- rate limits
  - disabling rate limiting [2-413](#)
  - enabling rate limiting [2-413](#)
  - setting [2-413](#)
- rcv-queues
  - mapping CoS values [2-618](#)
  - returning to default values [2-621](#)

- setting drop threshold [2-623](#)
- setting ratio limit [2-620](#)
- specifying maximum threshold [2-621](#)
- real servers
  - changing active connections [2-383](#)
  - limiting active connections [2-383](#)
  - new connections
    - defining defaults [2-625](#)
    - defining number of SYNs [2-625](#)
- reboots
  - restoring bindings across [2-191](#)
- receive queues
  - See [rcv-queues](#)
- receiving back channel
  - configuring [2-1238](#)
  - removing [2-1238](#)
- recovering a file [2-1248](#)
- redundancy
  - displaying
    - information [2-1053](#)
    - RF client list [2-1053](#)
    - RF operational counters [2-1053](#)
    - RF states [2-1053](#)
  - fast software upgrade [2-628](#)
  - reloading entire switch [2-629](#)
  - route processor
    - synchronizing BOOTVAR [2-10](#)
    - synchronizing BOOTVAR and configuration register default settings [2-10](#)
    - synchronizing configuration register [2-10](#)
    - synchronizing startup config [2-10](#)
  - setting mode [2-542](#)
  - synchronizing supervisor engines [2-626](#)
  - turning off auto synchronization [2-10](#)
- reflexive NDR
  - disabling shortcuts in TCAM [2-438](#)
  - enabling shortcuts in TCAM [2-438](#)
- regex
  - See [regular expression library](#)
- regular expression library
  - acknowledgments for open-source software [B-1](#)
- related documentation [xxvi](#)
- relationship between duplex and speed commands [2-1169](#)
- reloading switch [2-629](#)
- remote access
  - supervisor engines [2-8](#)
- remote command
  - executing directly to module [2-631](#)
  - executing directly to route processor [2-631](#)
- remote login [2-632](#)
- remote procedure call
  - See [RPC](#)
- remote SPAN
  - See [RSPAN](#)
- removing an interface from a channel group [2-22](#)
- replication mode
  - disabling [2-431](#)
  - enabling [2-431](#)
- Reverse Path Forwarding
  - See [RPF](#)
- RFC 1340 [2-785](#)
- RFC 1757, RMON alarm group
  - setting alarm [2-638](#)
- RFC 1757, RMON MIB [2-639](#)
  - RMON event table
    - adding event [2-640](#)
    - removing event [2-640](#)
- RGMP
  - disabling [2-302](#)
  - enabling [2-302](#)
- RM
  - configuring
    - purging time [2-364](#)
  - configuring purging interval [2-364](#)
  - disabling purging time [2-364](#)
- RMON
  - adding events [2-640](#)
  - alarms, disabling [2-638](#)

- alarms, enabling 2-638
  - disabling 2-640
  - disabling MIB object alarms 2-638
  - removing events 2-640
  - setting alarms on MIB objects 2-638
  - ROM, booting automatically 2-15
  - ROMMON
    - displaying status 2-1056
    - field upgrading 2-1252
    - programing new ROMMON into Flash 2-1252
    - setting execution preference 2-1252
  - ROM monitor mode,
    - summary 1-6
  - root guard
    - disabling 2-1139
    - displaying
      - root inconsistency status 2-1064
    - enabling 2-1139
  - routed MAC A-8
  - Route Processor Redundancy
    - See RPR
  - routing protocol packet
    - policing
      - controlling 2-486
  - routing protocol packet policing 2-486
  - RPC
    - displaying information 2-1057
  - RPF
    - disabling
      - exists-only checks 2-325
      - on an interface 2-323
      - triggered check 2-278
    - displaying
      - hardware information 2-933
      - triggered check events 2-864
    - enabling
      - exists-only checks 2-325
      - on an interface 2-323
    - setting
      - check interval 2-280
      - PIM back-off interval 2-278
      - triggered check interval 2-278
  - RSPAN
    - adding interfaces or VLANs 2-555
    - deleting interfaces or VLANs 2-555
    - deleting session 2-555
    - displaying
      - session information 2-1002
    - displaying list 2-1109
    - starting new session 2-555
  - RSTP+
    - configuring link type 2-1140
  - running configuration
    - displaying current operating information 2-1059
- 
- ## S
- sampled NetFlow
    - disabling
      - globally 2-534
      - on an interface 2-453
    - displaying status 2-985
    - enabling
      - globally 2-534
      - on an interface 2-453
    - specifying
      - sampling method 2-534
  - sanity check results, displaying 2-689
  - saving configuration changes 1-11
  - scheduled switchover
    - disabling 2-108, 2-109
    - enabling 2-108, 2-109
  - SCP
    - disabling
      - fast retry 2-585
    - displaying information 2-1061
    - enabling
      - fast retry 2-585

- setting
  - fast-retry interval [2-585](#)
- Secure Sockets Layer
  - See SSL
- See PVL
- See RM
- sending back channel
  - configuring [2-1240](#)
  - removing [2-1240](#)
- server load balancing
  - See SLB
- service module
  - disabling session [2-555](#)
  - enabling session [2-555](#)
- setting trusted port state [2-484, 2-503](#)
- shaped round robin
  - See SRR
- show [2-937](#)
- show commands
  - filter [1-7](#)
  - search [1-7](#)
- simulating a link-up condition [2-154](#)
- single-character patterns
  - special characters, table [1-8](#)
- SLB
  - displaying inband packet count [2-722](#)
- SNMP
  - disabling
    - authorization traps during unknown context error [2-1129](#)
    - linkdown during a switch failover [2-1130](#)
    - transceiver traps [2-1124](#)
  - displaying
    - interface index identification numbers [2-1062](#)
  - enabling
    - authorization traps during unknown context error [2-1129](#)
    - linkdown during a switch failover [2-1130](#)
    - transceiver traps [2-1124](#)
- ifIndex persistence
  - clearing previously interface configuration mode SNMP ifIndex commands [2-1118](#)
  - disabling globally [2-1125](#)
  - disabling on an interface [2-1120](#)
  - enabling globally [2-1125](#)
  - enabling on an interface [2-1120](#)
- informs
  - disabling [2-1122](#)
  - enabling [2-1122](#)
- removing source designation [2-1127](#)
- specifying
  - source interface
    - SNMP
      - specifying inform source designation [2-1127](#)
  - trap source designation [2-1127](#)
- traps
  - disabling [2-1122](#)
  - enabling [2-1122](#)
- Softfloat
  - acknowledgments for open-source software [B-1](#)
- softlink
  - disabling [2-154](#)
  - enabling [2-154](#)
- source-only timers
  - returning to default settings [2-239](#)
  - setting periodic flooding of multicast packets [2-239](#)
- source specific multicast
  - See SSM
- SPAN
  - disabling
    - service module session [2-555](#)
  - displaying
    - destination port permit list [2-1001](#)
    - session information [2-1002](#)
  - enabling
    - service module session [2-555](#)
  - service module session

- disabling [2-555](#)
  - enabling [2-555](#)
- SPAN destination port permit list [2-553](#)
- displaying [2-1001](#)
- spanning tree
  - active states
    - displaying [2-1064](#)
  - configuring link type [2-1140](#)
  - disabling
    - BackboneFast [2-1131](#)
    - BPDU filtering [2-1132](#)
    - BPDU guard [2-1134](#)
    - extended system ID display [2-1138](#)
    - loop guard as a default [2-1141](#)
    - loop guard mode [2-1139](#)
    - PortFast BPDU filtering [2-1158](#)
    - PortFast BPDU guard [2-1160](#)
    - PortFast by default [2-1161](#)
    - PortFast by default on all access ports [2-1161](#)
    - PortFast on an interface [2-1156](#)
    - root guard mode [2-1139](#)
  - displaying
    - active interfaces only [2-1064](#)
    - active states [2-1064](#)
    - BackboneFast status [2-1064](#)
    - bridge status and configuration [2-1064](#)
    - default path cost method [2-1064](#)
    - status information [2-1064](#)
    - status per VLAN [2-1064](#)
    - summary of interface information [2-1064](#)
    - UplinkFast status [2-1064](#)
  - enabling
    - BackboneFast [2-1131](#)
    - BPDU filtering [2-1132](#)
    - BPDU guard [2-1134](#)
    - extended system ID display [2-1138](#)
    - loop guard as a default [2-1141](#)
    - loop guard mode [2-1139](#)
    - PortFast BPDU filtering [2-1158](#)
    - PortFast BPDU guard [2-1160](#)
    - PortFast by default [2-1161](#)
    - PortFast by default on all access ports [2-1161](#)
    - PortFast on an interface [2-1156](#)
    - root guard mode [2-1139](#)
- EtherChannel
  - guard misconfiguration detection [2-1136](#)
- interface
  - portfast mode, disabling [2-1156](#)
  - portfast mode, enabling [2-1156](#)
- path cost
  - reverting to default [2-1135](#)
  - setting [2-1135](#)
- port priority
  - reverting to default [2-1162](#)
  - setting [2-1162](#)
- restarting protocol migration [2-84](#)
- setting default pathcost calculation method [2-1155](#)
- specifying
  - transmit hold count [2-1163](#)
- UplinkFast
  - disabling [2-1164](#)
  - enabling [2-1164](#)
- VLANs
  - configuring [2-1166](#)
  - reverting to defaults [2-1166](#)
- SPAN session
  - adding interfaces or VLANs [2-555](#)
  - deleting interfaces or VLANs [2-555](#)
  - deleting session [2-555](#)
  - starting new session [2-555](#)
- special characters
  - anchoring, table [1-10](#)
- SP QoS manager
  - See QM-SP
- SRM with SSO
  - configuring
    - route converge delay time interval [2-642](#)
  - setting redundancy mode [2-542](#)

- SRR queues
  - configuring
    - bandwidth [2-1291](#)
- SSL
  - shutting down [2-153](#)
- SSM mapping [2-240](#)
  - configuring
    - static mapping database [2-240](#)
  - disabling [2-240](#)
  - enabling [2-240](#)
- SSO
  - configuring
    - route converge delay time interval [2-642](#)
    - setting redundancy mode [2-542](#)
- Stateful Switch Over
  - See SSO
- static MAC address entries
  - clearing [2-63](#)
- statistics data export
  - See MLS QoS statistics data export
- statistics retrieval
  - setting interval [2-646](#)
- sticky ARP
  - disabling
    - global [2-306](#)
    - per-interface [2-308](#)
  - enabling
    - global [2-306](#)
    - per-interface [2-308](#)
- sticky MACs
  - enabling [2-1200](#)
  - removing [2-1200](#)
- sticky port
  - deleting [2-82](#)
- storm control
  - disabling suppression mode [2-1178](#)
  - enabling suppression mode [2-1178](#)
  - setting suppression level [2-1178](#)
- strict-priority queue
  - mapping CoS values [2-606](#)
- stub
  - enabling non-RPF multicast fastdrop [2-433](#)
- subinterface configuration mode, summary [1-6](#)
- sup-bootflash
  - displaying file system information [2-1075](#)
- switch console, accessing [2-632](#)
- switching, NetFlow
  - clearing statistics [2-48](#)
  - setting cache size [2-204](#)
- switching characteristics
  - disabling
    - capture mode [2-1189](#)
    - Flexlink [2-1186](#)
  - enabling
    - capture function [2-1189](#)
    - Flexlink [2-1186](#)
  - excluding from link-up calculation [2-1184](#)
  - modifying [2-1180, 2-1182, 2-1184](#)
    - capture function [2-1191](#)
  - optimizing port configuration for host connection [2-1180](#)
  - returning to interfaces
    - capture function [2-1180, 2-1184](#)
- switching interface
  - displaying administrative and operational status [2-764](#)
  - displaying Flexlink pairs [2-766](#)
- Switch-Module Configuration Protocol
  - See SCP
- switch ports
  - clearing
    - VLAN mapping per port [2-1212](#)
  - configuring
    - capture ports [2-1189](#)
    - VLAN mapping per port [2-1212](#)
    - voice VLANs [2-1217](#)
  - defining
    - PVLAN association [2-1206](#)
  - disabling

- VLAN mapping per port [2-1215](#)
- enabling
  - VLAN mapping per port [2-1215](#)
- mapping
  - PVLANS for promiscuous port [2-1207](#)
- modifying characteristics [2-1180](#)
- port security
  - configuring aging time [2-1198](#)
  - configuring aging type [2-1198](#)
  - disabling [2-1197](#)
  - displaying setting information [2-1042](#)
  - enabling [2-1197](#)
  - removing MAC address from list [2-1200](#)
  - setting maximum number of secured addresses [2-1202](#)
  - setting violation action [2-1204](#)
  - violation actions [2-1204](#)
- preventing packet forwarding [2-1188](#)
- removing
  - mapping PVLANS for promiscuous port [2-1207](#)
  - PVLAN mapping [2-1206](#)
  - voice VLAN [2-1217](#)
- setting
  - mode [2-1195](#)
  - trunk characteristics [2-1209](#)
  - VLAN in access mode [2-1182](#)
  - specifying destination VLANs [2-1191](#)
- switch reload [2-629](#)
- synchronizing supervisor engines [2-626](#)
- system images
  - default filename [2-15](#)
- system prompts [1-6](#)
- systems
  - configuring FIFO overflow error count [2-1220](#)
- system software
  - booting [2-15](#)
  - displaying names and sources of configuration files [2-1091](#)
  - displaying uptime since active [2-1091](#)
  - displaying version of [2-1091](#)

---

**T**

- Tab key
  - command completion [1-1](#)
- table contention level
  - See TCL
- tables
  - characters with special meaning [1-8](#)
  - class syntax description [2-587, 2-593](#)
  - common keyword aliases to URLs [2-94](#)
  - CoS-to-DSCP mapping table [2-467](#)
  - default bandwidth values [2-1281](#)
  - default MTU values [2-569](#)
  - DSCP-to-CoS default mapping table [2-470](#)
  - DSCP-to-EXP default mapping table [2-472](#)
  - ERSPAN destination session configuration mode syntaxes [2-561](#)
  - ERSPAN source session configuration mode syntaxes [2-562](#)
  - EXP-to-DSCP default mapping table [2-475](#)
  - EXP-to-EXP mutation default mapping table [2-476](#)
  - fsck utility checks and actions [2-144](#)
  - group syntax description [2-28](#)
  - IP-Precedence-to-DSCP default mapping [2-478](#)
  - mac access-list extended subcommands [2-362](#)
  - match syntax description [2-27, 2-28](#)
  - MFIB forwarding entries and interface flags [2-868](#)
  - MFIB platform flags [2-872](#)
  - relationship between duplex and speed commands [2-126, 2-1170](#)
  - show cable-diagnostics tdr command output fields [2-672](#)
  - show cdp neighbors detail field descriptions [2-677](#)
  - show cdp neighbors field descriptions [2-676](#)
  - show environment status command output fields [2-704](#)
  - show environment temperature command output fields [2-707](#)
  - show interfaces accounting command output fields [2-746](#)
  - show ip cache flow command output fields—current flow [2-788](#)

- show ip cache flow command output fields—flow switching cache [2-787](#)
- show ip cache flow command output fields—NetFlow activity by protocol [2-787](#)
- show ip cache flow command output fields—packet size distribution [2-786](#)
- show ip cache verbose flow field descriptions in activity by protocol display [2-791](#)
- show ip cache verbose flow field descriptions in the NetFlow cache display [2-790](#)
- show ip cef inconsistency field descriptions [2-796](#)
- show ip dhcp snooping command output [2-803](#)
- show ip igmp groups field descriptions [2-810](#)
- show ip interface field descriptions [2-822, 2-891](#)
- show ip mcache field descriptions [2-824](#)
- show ip mds interface field descriptions [2-826](#)
- show ip mpacket field descriptions [2-828](#)
- show ip mroute field descriptions [2-818, 2-831](#)
- show ip msdp count field descriptions [2-837](#)
- show ip msdp peer field descriptions [2-839](#)
- show ip msdp sa-cache field descriptions [2-841](#)
- show ip msdp summary field descriptions [2-842](#)
- show ip pim bsr field descriptions [2-846](#)
- show ip pim mdt bgp field descriptions [2-849](#)
- show ip pim mdt history field descriptions [2-850](#)
- show ip pim mdt receive field descriptions [2-851](#)
- show ip pim mdt send field descriptions [2-853](#)
- show ip pim neighbor field descriptions [2-854](#)
- show ip pim rp-hash field descriptions [2-857](#)
- show ip pim rp mapping field descriptions [2-859](#)
- show ipv6 mfib active field descriptions [2-870](#)
- show ipv6 mfib count field descriptions [2-871](#)
- show ipv6 mfib field descriptions [2-869](#)
- show ipv6 mfib verbose field descriptions [2-872](#)
- show ip wccp web-cache detail command output fields [2-866](#)
- show lacp command output fields [2-880](#)
- show memory dead field descriptions [2-894](#)
- show mls cef command output fields [2-901, 2-916](#)
- show mls cef summary command output fields [2-935](#)
- show mpls l2transport vc command field descriptions [2-1007](#)
- show policy-map control-plane field descriptions [2-1039](#)
- show port flowcontrol command output fields [2-757](#)
- show spanning-tree command output fields [2-1065](#)
- show spanning-tree vlan command output fields [2-1068](#)
- show team counts command output fields [2-1080](#)
- show version field descriptions [2-1092](#)
- show vlan command output fields [2-1096](#)
- show vlan private-vlan command output fields [2-1108](#)
- show vlans command output fields [2-1111](#)
- show vtp command output fields [2-1115](#)
- special characters
  - multipliers, table [1-9](#)
  - used for anchoring [1-10](#)
- speed command options [2-1168](#)
- supported duplex command options [2-125](#)
- supported speed command options [2-1169](#)
- time-based sampling intervals [2-534](#)
- URL prefix aliases for local writable storage file systems [2-95](#)
- URL prefix aliases for network file systems [2-95](#)
- URL prefix aliases for special file systems [2-95](#)
- valid cluster numbers [2-146](#)
- valid interface types [2-157](#)
- TAC
  - displaying information [2-1084](#)
- tag-to-tag load balancing
  - disabling [2-567](#)
  - enabling [2-567](#)
- TCAM
  - ACLs
    - clearing match counters [2-65](#)
    - setting default action during update [2-395](#)
  - clearing
    - ACL match counters [2-65](#)
  - disabling
    - optimization for IPv6 ACLs [2-583](#)
    - sharing of global default ACLs [2-396](#)

- shortcuts [2-438](#)
- displaying
  - interface-based information [2-1081](#)
  - protocol-based information [2-1081](#)
  - statistical information [2-1079](#)
- enabling
  - optimization for IPv6 ACLs [2-583](#)
  - sharing of global default ACLs [2-396](#)
  - shortcuts [2-438](#)
- prioritizing interfaces [2-1223](#)
- setting
  - default action during update [2-395](#)
- update
  - setting default action [2-395](#)
- TCAM ACL match counters, clearing [2-65](#)
- TCL
  - displaying MLS information [2-988](#)
- TDR
  - clearing
    - all interfaces [2-33](#)
    - specific interface [2-33](#)
  - displaying cable diagnostic test results [2-671](#)
  - running cable diagnostics [2-1225](#)
- temperature readings
  - displaying information [2-706](#)
- Ternary Content Addressable Memory
  - See TCAM
- time-based ACLs
  - configuring
    - time ranges [2-1227](#)
  - enabling [2-1227](#)
  - removing
    - time limitation [2-1227](#)
- time domain reflectometry
  - See TDR
- time-range command [2-1227](#)
- TopN
  - clearing reports [2-86](#)
  - configuring
    - sampling interval [2-90](#)
    - sorting by statistic type [2-90](#)
  - enabling
    - processes and reports [2-90](#)
- traceroute MAC
  - displaying
    - by interface [2-1229](#)
    - source IP to destination IP [2-1229](#)
    - source MAC to destination MAC [2-1229](#)
- tracking
  - configuring
    - designated router [2-1175](#)
  - configuring interface [2-1233](#)
  - entering tracking configuration mode [2-1233](#)
  - removing tracking [2-1233](#)
- transceiver
  - disabling
    - monitoring [2-1235](#)
  - enabling
    - monitoring [2-1235](#)
- transceivers
  - disabling
    - traps [2-1124](#)
  - displaying
    - operational information [2-768](#)
    - threshold violations [2-768](#)
  - enabling
    - traps [2-1124](#)
- transmit hold count
  - spanning tree
    - specifying [2-1163](#)
- transmit-queue
  - setting size ratio [2-1287](#)
- traps, enabling [2-1122](#)
- troubleshooting
  - displaying information [2-1084](#)
- trunk characteristics
  - adding VLANs [2-1209](#)
  - displaying information [2-771](#)

- removing VLANs [2-1209](#)
- resetting to defaults [2-1209](#)
- setting [2-1209](#)
- two-way VLANs
  - displaying [2-1107](#)

---

## U

### UDE

- displaying
  - operational status [2-774](#)
- software based
  - configuring [2-1250](#)
  - removing configuration [2-1250](#)

### UDLD

- aggressive mode
  - disabling globally on fiber interfaces only [2-1242](#)
  - disabling on an interface [2-1244](#)
  - enabling globally on fiber interfaces only [2-1242](#)
  - enabling on an interface [2-1244](#)
- disabling
  - on interface [2-1244](#)
- global configuration mode
  - enabling on fiber interfaces only [2-1242](#)
- interface configuration mode
  - enabling on interface [2-1244](#)
- resetting all ports shut down by UDLD [2-1246](#)

### UDLR

- changing UDP port numbers [2-1247](#)
- configuring
  - GRE tunnel as a message-sending back channel [2-1240](#)
  - GRE tunnel as a receiving back channel [2-1238](#)
- displaying
  - information [2-819](#)
- enabling
  - forwarding of ARP and NHRP [2-1236](#)
- removing
  - GRE tunnel receiving back channel [2-1238](#)

- GRE tunnel sending back channel [2-1240](#)

### UDP

- changing port numbers [2-1247](#)
- configuring
  - CASA queue length [2-183](#)

### UDP datagrams

- disabling flooding [2-217](#)
- flooding using spanning-tree algorithm [2-217](#)
- UDP checksums on all outgoing packets [2-217](#)

### unicast entries

- fast-aging time
  - configuring [2-397](#)
  - restoring to defaults [2-397](#)
- long-aging time
  - configuring [2-398](#)
  - restoring to defaults [2-398](#)
- normal-aging time
  - configuring [2-399](#)
  - restoring to defaults [2-399](#)

### unicast RPF

- See uRPF

### unidirectional Ethernet

- See UDE

### unidirectional link

- See UDLR

### unidirectional link routing

- See UDLR

### unidirectional transceiver

- displaying
  - type [2-760](#)
  - displaying operational state [2-774](#)

### unknown unicast flood blocking

- See UUFb

### unknown unicast traffic, preventing [2-1188](#)

### uRPF

- disabling
  - exists-only checks [2-325](#)
  - hardware when RPF ACL enabled [2-414](#)
- enabling

- exists-only checks [2-325](#)
- hardware when RPF ACL enabled [2-414](#)
- user EXEC mode, summary [1-6](#)
- usernames
  - configuring [2-1254](#)
  - setting password [2-1254](#)
  - setting privilege level [2-1254](#)
- UUFB
  - switch ports
    - preventing packet forwarding [2-1188](#)

---

## V

### VACL logging

- configuring
  - logging parameters [2-1264](#)
  - logging threshold [2-1264](#)
  - log table size [2-1264](#)
  - parameters [2-1264](#)
  - redirect packet rate [2-1264](#)
- displaying
  - configuration information [2-1097](#)
  - flow table contents [2-1097](#)
  - logging property information [2-1097](#)
- log table size [2-1264](#)
- redirect packet rate [2-1264](#)
- returning to default logging values [2-1264](#)
- returning to default values [2-1264](#)
- threshold [2-1264](#)

### VACLs

- applying VLAN access maps [2-1272](#)
- creating
  - VLAN access map [2-1266](#)
- defining extended MAC access lists [2-361](#)
- disabling capture function [2-1189](#)
- enabling capture function [2-1189](#)
- entering
  - VLAN access-map mode [2-1266](#)
- packet action

- dropping [2-2](#)
- forwarding [2-2](#)
- redirecting [2-2](#)
- setting [2-2](#)
- specifying
  - access-map sequence [2-380](#)
  - match clause [2-380](#)
- value mask result
  - See VMR
- VFI
  - creating [2-341](#)
  - entering manual configuration mode [2-341](#)
- virtual forwarding instance
  - See VFI [A-10](#)
- Virtual Private LAN Service
  - See VPLS
- VLAN 1 minimalization
  - command [2-1209](#)
  - usage guideline [2-1210](#)
- VLAN access control lists
  - See VACL
- VLAN access-map command mode
  - entering [2-1266](#)
- VLAN database
  - entering [2-1268](#)
  - resetting [2-635](#)
- VLAN link-up calculation
  - excluding a switch port [2-1184](#)
  - including a switch port [2-1184](#)
- VLAN mapping per port
  - clearing [2-1212](#)
  - configuring [2-1212](#)
  - disabling [2-1215](#)
  - displaying
    - 802.1Q VLAN to ISL VLAN mapping [2-1106](#)
    - mapping status [2-776](#)
  - enabling [2-1215](#)
- VLANs
  - adding

- global configuration mode [2-1262](#)
  - applying an ARP ACL [2-167](#)
  - clearing
    - counters [2-87](#)
    - DAI statistics [2-42](#)
    - hardware logic [2-39](#)
  - configuring
    - ARE hops [2-1258](#)
    - backup CRF mode [2-1258](#)
    - bridging characteristics [2-1258](#)
    - config-VLAN submode [2-1258](#)
    - FDDI ring number [2-1258](#)
    - internal allocation scheme [2-1274](#)
    - media type [2-1258](#)
    - MTU size [2-1258](#)
    - parent VLAN ID [2-1258](#)
    - SAID identifier [2-1258](#)
    - state [2-1258](#)
    - STP type [2-1258](#)
    - Token Ring number [2-1258](#)
    - translational ID [2-1258](#)
    - VLAN name [2-1258](#)
  - config-VLAN submode
    - configuring [2-1258](#)
    - deleting [2-1258](#)
    - entering [2-1258](#)
    - specifying RSPAN [2-1258](#)
  - deleting
    - config-VLAN submode [2-1258](#)
    - global configuration mode [2-1262](#)
  - disabling
    - dot1q tagging [2-1270](#)
  - disabling DAI [2-176](#)
  - displaying
    - CEF information [2-798](#)
    - CEF next-hop information [2-798](#)
    - Cisco IOS VLAN subinterface information [2-1110](#)
    - configuration information [2-1097](#)
    - current operating information [2-1059](#)
    - DAI status [2-777](#)
    - dot1q tagging information [2-1101](#)
    - filter information [2-1102](#)
    - flow table contents [2-1097](#)
    - internal VLAN allocation information [2-1104](#)
    - internal VLAN status [2-1093](#)
    - Layer 2 VLAN information [2-1093](#)
    - logging property information [2-1097](#)
    - number of logical virtual ports required [2-1112](#)
    - per port mapping [2-1106](#)
    - RSPAN VLANs [2-1109](#)
    - software-cached counter values [2-1100](#)
    - total number of interface VLANs [2-762](#)
    - twoway [2-1107](#)
    - workaround VLANs [2-1104](#)
  - enabling
    - dot1q tagging [2-1270](#)
  - enabling DAI [2-176](#)
  - entering configuration mode [2-1262](#)
  - entering configuration submode [2-1268](#)
  - erasing the VLAN database configuration file [2-130](#)
  - implementing database [2-4](#)
  - implementing new database [2-4](#)
  - incrementing configuration number [2-4](#)
  - mapping to ISL VLANs [2-1276](#)
  - mapping to MST instance [2-155](#)
  - removing ISL VLAN mapping [2-1276](#)
  - restarting local traffic [2-1117](#)
  - shutting down internally [2-1260](#)
  - shutting down local traffic [2-1117](#)
- VLAN translation
- configuring
    - mapping per port [2-1212](#)
  - disabling
    - VLAN mapping per port [2-1215](#)
  - enabling
    - VLAN mapping per port [2-1215](#)
  - supported modules [2-1212](#)
- VMR

- acronym for value mask result
- voice VLANs
  - configuring on switch ports [2-1217](#)
  - removing
    - from switch ports [2-1217](#)
- VPLS
  - configuring VPN ID [2-341](#)
  - creating Layer 2 VFIs [2-341](#)
  - entering L2 VFI configuration mode [2-341](#)
- VRF
  - configuring
    - default group [2-389](#)
    - group address ranges [2-388](#)
  - disabling
    - recording of data MDT reuse [2-390](#)
  - displaying
    - non-default entries [2-937](#)
  - enabling
    - recording of data MDT reuse [2-390](#)
- VTP
  - displaying
    - domain information [2-1114](#)
    - statistics information [2-1114](#)
  - global configuration mode
    - setting domain name [2-1278](#)
    - setting IFS file [2-1278](#)
    - setting mode [2-1278](#)
    - setting preferred updater ID source [2-1278](#)
  - pruning
    - disabling [2-1278](#)
    - enabling [2-1278](#)
  - setting
    - client mode [2-1278](#)
    - domain name [2-1278](#)
    - IFS file system [2-1278](#)
    - preferred updater ID source [2-1278](#)
    - server mode [2-1278](#)
    - transparent mode [2-1278](#)
    - version [2-1278](#)

- specifying
  - password [2-1278](#)
- VTP domain
  - linking [2-533](#)
  - removing [2-533](#)

---

## W

- WAN
  - disabling
    - 802.1Q transparency [2-586](#)
  - enabling
    - 802.1Q transparency [2-586](#)
- watch list
  - adding IP address [2-181](#)
  - clearing entries [2-43](#)
  - configuring [2-181](#)
  - disabling [2-181](#)
  - displaying [2-782](#)
  - enabling [2-181](#)
  - setting
    - maximum login attempts [2-179](#)
- WCCP
  - disabling
    - IP multicast packet reception [2-327](#)
    - mask assignment hardware acceleration [2-331](#)
    - packet redirection [2-329](#)
  - displaying
    - global statistics [2-865](#)
    - inband packet count [2-722](#)
  - enabling
    - IP multicast packet reception [2-327](#)
    - mask assignment hardware acceleration [2-331](#)
    - packet redirection [2-329](#)
- Web Cache Coprocessor Protocol
  - See WCCP
- weighted random early detection
  - See WRED
- weighted round robin

- See WRR
  - Wireless LAN Services Module
    - See WLSM
  - wireless network
    - configuring mGRE tunnels [2-540](#)
    - displaying information [2-996](#)
  - WLSM
    - configuring
      - mobility [2-540](#)
      - wireless mGRE tunnels [2-540](#)
    - displaying information [2-996](#)
    - specifying
      - convert NBMA to BMA [2-540](#)
      - network ID [2-540](#)
  - workaround VLANs [2-1104](#)
  - WRED
    - specifying maximum threshold [2-1289](#)
  - write erase command
    - See erase command [2-130](#)
  - WRR
    - queue mapping
      - CoS to drop thresholds [2-1285](#)
      - DSCP to drop thresholds [2-1286](#)
    - returning to default queue values [2-1289](#)
    - setting transmit queue size ratio [2-1287](#)
  - WRR queues
    - configuring
      - bandwidth [2-1281](#)
    - specifying maximum threshold [2-1289](#)
- 
- ×
- XL mode
    - definition [2-401](#)
    - support modules [2-401](#)